ORDER FOR SUPPLIES AND SERVICES				IMPORTANT: See instructions in GSAR 553.370-300-1 for distribution			PAGE 1 OF 1 PAGE(S)
1. DATE OF ORDER 10/05/2012		2. ORDER NUMBER GST0313DS0001		3. CONTRACT NUMBER GS00Q09BGD0012			4. ACT NUMBER A2473651Q
FOR GOVERNMENT USE ONLY	5. ACCOUNTING CLASSIFICATION				6. FINANCE DIVISION		
	FUND 299X	ORG CODE A03VR110	B/A CODE F1	O/C CODE 25	AC	SS	VENDOR NAME
	FUNC CODE C01	C/E CODE H08	PROJ./PROS. NO.	CC-A	MDL	FI	G/L DEBT
	W/ITEM	CC-B	PRT./CRFT		AI	LC	DISCOUNT

7. TO: CONTRACTOR *(Name, address and zip code)*	8. TYPE OF ORDER B. DELIVERY	REFERENCE YOUR
Terrance Hobson APPTIS INC 4800 Westfields Blvd STE 1 CHANTILLY, VA 20151-2293 United States (703) 279-5449	Please furnish the following on the terms specified on both sides of the order and the attached sheets, if any, including delivery as indicated.	
	This delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above numbered contract.	
	C. MODIFICATION NO. 000 TYPE OF MODIFICATION:	AUTHORITY FOR ISSUING

9A. EMPLOYER'S IDENTIFICATION NUMBER 541251160	9B. CHECK, IF APPROP WITHHOLD 20%	Except as provided herein, all terms and conditions of the original order, as heretofore modified, remain unchanged.
10A CLASSIFICATION B. Other than Small Business		10B TYPE OF BUSINESS ORGANIZATION C. Corporation

11. ISSUING OFFICE *(Address, zip code, and telephone no.)*	12. REMITTANCE ADDRESS *(MANDATORY)*	13. SHIP TO*(Consignee address, zip code and telephone no.)*
GSA Region 3 Debra L tuart 20 NORTH EIGHTH STREET PHILADELPHIA, PA 19107-3191 United States (215) 446 5817	APPTIS INC P O Box 8500 1686 Philadelphia,PA 19178-1686 United States	Robert J Bolluyt 7700 Arlington Blvd Suite 5101 Falls Church, VA 22042 United States 011-49-6371-9464-7370

14 PLACE OF INSPECTION AND ACCEPTANCE	15 REQUISITION OFFICE *(Name, symbol and telephone no)*
Beau Kiser 7700 Arlington Blvd Suite 5101 Falls Church, VA 22042 United tates	Allen Cardwell GSA Region 3 20 North 8th Street Philadelphia, PA 19107 United States (215) 446-5831

16. F.O.B. POINT	17. GOVERNMENT B/L NO.	18. DELIVERY F.O.B. POINT ON OR BEFORE	19. PAYMENT/DISCOUNT TERMS
Destination		10/27/2013	NET 30 DAYS / 0.00 % 0 DAYS / 0.00 % 0 DAYS

20. SCHEDULE

Task Order GST0313DS0001 for TRICARE MANAGEMENT ACTIVITY Military Health System Cyberinfrastructure Services (MCiS) Network Engineers and Specialists (NE&S), incorporates the Performance Work Statement dated August 24, 2012 under ITSS Control #ID03120052 and accepts the Contractor's quote submitted on September 4, 2012. The total ceiling price of this task order is $(b) (4) 5 for a 12- month base period and four 12-month option periods inclusive of optional items.

The base period of performance for this task order is 10/28/2012 through 10/27/2013. Subject to provisions of 52.232-18 (see below), this task order is hereby awarded as a hybrid Firm Fixed Price/Labor Hour/Cost Reimbursement type task order The total ceiling price of the base period of performance (inclusive of optional items) is (b) (4) . Line item breakdown is as follows (note ITSS system item structure currently consists of 3 items only, combining OPTIONAL Items 0002 AND 0003 within Item 0002, please refer to the description):

(b) (4)

Order is FUNDED IN THE AMOUNT OF (b) (4)

In accordance with FAR clause 52.232-18 Subject to Availability of Funds (Apr 1984) Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer

12/19/2012 Note: Henceforth all references to 'TRICARE Management Activity (TMA)' throughout this document should be interpreted as 'Defense Health Agency (DHA)'

TRICARE MANAGEMENT ACTIVITY
Military Health System Cyberinfrastructure Services (MCiS)
Network Engineers and Specialists (NE&S)

PERFORMANCE WORK STATEMENT

NE&S - Table of PWS Revisions

Rev. No.	Revision Date	Name	Description	Task Order Amend/Mod #
1	8/16/2012	A Cardwell	**4.6 Deliverable / Delivery Schedule –** Changed Deliverable 7 to be completed 30 DACA **2.1.8 Quality Control Plan – Deliverable 8 –** Removed the requirement to provide the QCP with quote. **ATTACHMENT E - JOB TITLE: *Senior Network Engineer for CONUS*** – removed references to Pacific Region **2.1.1.2 Monthly Progress Report (MPR)** – Removed 'expenditures' from the list of items to be included in the Monthly Report. These are included in the 'cost' item. **2.1.6.1 Incoming Transition Plan** – added the requirement to evolve the transition plan over the course of the transition period. **ATTACHMENT E:** all position descriptions have been updated to reflect the correct security / ADP requirements **5.2 Other Direct Costs (ODCs)** – Added requirement for prior authorization by COR for all OCDs Changed language describing the list of ODC amount, indicating that they are estimates rather than 'not-to-exceed' totals. **2.1.15.3 & 2.1.15.3** – changed link references to access information regarding Europe and Germany **8.0 ATTACHMENTS Section Index:** (*added this index*) **8.0 ATTACHMENTS Section Index** – added **ATTACHMENT F - Instructions for Contractor Access to DoD IT Systems** **6.4.3 Personally Identifiable Information (PII) and Protected Health Information (PHI)** – revised complete section content **6.4.5 Business Associates –** revised complete section content **6.13 Clauses** – added the following clause: **SOFA CLAUSE: INVITED CONTRACTOR OR TECHNICAL REPRESENTATIVE STATUS UNDER U.S. - REPUBLIC OF**	Amend 4

			KOREA (ROK)	
2	8/24/2012	A Cardwell	**6.13 Clauses** – removed duplicated SOFA clause for Republic of Korea	Amend 5
3	12/04/2012	A Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement** **CONUS** **Air Force** Removed Hanscom AFB MA **OCONUS – Pacific** **Army** Changed Zama (CAMP) JP to Kadena JP **OCONUS – Europe** **Army** Added Bavaria GE **ATTACHMENT E: LABOR CATEGORY RESPONSIBILITIES AND REQUIRED QUALIFICATIONS** Changed **'JOB TITLE: *LAN (Network) Specialist (Landstuhl, Germany & Bavaria, Germany)'*** to include Bavaria	MOD001
4	12/07/2012	A Cardwell	**1.3 SCOPE (sub-sections B & D)** – revised to reflect correct staffing distribution based on changes made in MOD001 and MOD002 **ATTACHMENT A – Sites & Support Staff Requirement –** revised each regional total per changes made in MOD001 and MOD002 **CONUS** **Air Force** Removed Laughlin AFB TX & Randolph AFB TX **ARMY** Changed Carson, CO from 2 to 1 billet Correction – changed Knox from TN to KY **OCONUS – Pacific** Added **AIR FORCE** and moved Kadena from **ARMY** to **AIR FORCE** **ARMY** Added 2 site-funded billets to Korea bringing total Network Specialist billets to 3. **OCONUS – Europe** **Army**	MOD002

			Added note to Bavaria GE that the base location is Vilseck **2.1.16 ADP Sensitivity Designation Report** – added this report requirement. **2.1.6.2 Outgoing Transition Plan (Optional – To be exercised as a unilateral right of the Government) – Deliverable 6 -** clarification **4.6 Deliverable / Delivery Schedule –** added ADP Sensitivity Designation Report / Deliverable 13 **5.2.4 Points of Contact** - updated **6.13 Clauses –** Clarified the following clause: **'EXPORT CONTRACT ACT COMPLIANCE (DEC 2006)'** **2.1.6.2 Outgoing Transition Plan** – added statement that the Government will provide 30 days advanced notice to the contractor prior to exercising this option	
5	8/22/2013	A Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement** – Changed 'Ft. Richardson AK' to 'Joint Base - Elmendorf-Richardson AK' – The NE&S specialist will support the troop medical clinic as well as the medical treatment facility at this merged site – The OPCON for this position will switch from Ft. Wainwright AK to the CIO at Elmendorf hospital. Designated one of the 2 site-funded positions in Korea as a 'Systems and Network Specialist Total Onboard = 69	MOD006
6	12/19/2013	A Cardwell	**ATTACHMENT E: LABOR CATEGORY RESPONSIBILITIES AND REQUIRED QUALIFICATIONS –** added PD for '*Systems and Network Specialist. Yongsan (Seoul) Korea'* **ATTACHMENT E: LABOR CATEGORY RESPONSIBILITIES AND REQUIRED QUALIFICATIONS –** updated the **EDUCATION** section of all PD's to clarify requirements, including language specifying the need for any degree or certification to have been granted by a college, university, technical or vocational school that is accredited by a bona fide accrediting agency. **ATTACHMENT E: LABOR CATEGORY RESPONSIBILITIES AND REQUIRED QUALIFICATIONS –** added a PD for ***'Systems and Network Specialist (CONUS)'*** to support 2 positions being considered for Camp Pendleton.	MOD010

			ATTACHMENT E: LABOR CATEGORY RESPONSIBILITIES AND REQUIRED QUALIFICATIONS – revised language in '**OTHER SKILLS'** Section of PDs for '***Systems and Network Specialist (Sembach, Germany)***' and '***Systems and Network Specialist (Yongsan (Seoul) Korea)*** **6.13 Clauses –** added the **'CONTRACTOR MANPOWER REPORTING'** clause, including Requiring Activity and UIC code.	
7	01/03/2014	A. Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement** - Added 2 network specialist positions in Camp Pendleton – added over January and February 2014 ***Total Onboard = 71***	MOD012
8	06/11/2014	A. Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement** - Removed 1 Network Specialist positions at West Point – change effective 5/3/2014 ***Total Onboard = 70***	MOD013
9	08/14/2014	A. Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement** - 1. Add 0.5 FTE Network Specialist position for the Air Force at Pearl Harbor-Hickam (15th MDG), HI 2. Change the The Specialist at Tripler, HI to .5 FTE. The specialist in this role will split their time between Tripler and Pearl Harbor-Hickam. Change effective 8/18/2014 **5.2.4 Points of Contact –** updated contact information. ***Total Onboard = 70***	MOD014
10	10/21/2014	A. Garcia	**4.6 Deliverable / Delivery Schedule –** Changed Deliverable 12 - Semi-annual Inventory of equipment - to be completed NLT 01 FEB and 01 AUG of each year.	MOD017
11	12/05/2014	A. Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement** - 1. Removed 1 Network Specialist position at Fort Benning – this position was terminated effective 10/27/2014 2. The 3 Network Specialist positions at Camp Pendleton were reduced to 2 effective 10/28/2014, and will go down to 1 effective 12/27/2014. This modification will remove the SAF status on the OY2 funding	MOD018

`			**1.3 Scope –** reduced staffing totals accordingly ***Total Onboard = 67 (effective 12/27/2014)***	
12	2/13/2015	A. Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement –** • Added 1 Network Specialist position at Fort Riley KS – effective 2/28/2015 • Under OCONUS Air Force – dropped Pearl Harbor-Hickam 15th MDG (0.5) – moved this 0.5 Network Specialist position to Army Tripler which becomes 1.0 Network Specialist **4.6 Deliverable / Delivery Schedule –** Changed Deliverable 12 - Semi-annual Inventory of Equipment - to be completed NLT 15 February and 15 August of each year **1.3 Scope –** adjusted staffing totals based on updated **ATTACHMENT A**	MOD019
13	7/6/2015	A. Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement –** • Added DNOC San Antonio to CONUS locations, and added four (4) Network Specialists positions to this site – effective ASAP but not before a valid CAC card can be issued. • Added GAL Auburn WA to CONUS locations, and added one (1) Network Specialist position, and one (1) Network Engineer position to this site – effective ASAP but not before a valid CAC card can be issued. • Added Fairchild AFB WA to CONUS Air Force locations, and added one (1) Network Specialist position to this site – effective ASAP but not before a valid CAC card can be issued. • Added Oak Harbor WA to CONUS Navy locations, and added one (1) Network Specialist position to this site – effective ASAP but not before a valid CAC card can be issued. *<added a total of 8 positions>* **1.3 Scope –** adjusted staffing totals based on revisions to **ATTACHMENT A** ***Total Onboard = 76 (effective 6/29/2015)***	MOD020

14	4/14/2016	A. Cardwell	**ATTACHMENT A – Sites & Support Staff Requirement** • Changed PD for Network Specialist GAL Auburn WA to 'Systems and Network Specialist CONUS' • Added 11 CONUS based Network Specialist & USAF / USN Locations **1.3 Scope –** adjusted staffing totals based on revisions to **5.2.4 Points of Contact** Replaced Anthony Heath with Ronald Locker as DHA HIT IOD Contracting Officer's Representative (COR) – Europe	MOD024
15	10/20/2016	A. Cardwell	**5.2.4 Points of Contact -** Updated POC Information **ATTACHMENT A – Sites & Support Staff Requirement** Add Shaw AFB with one network specialist, and decremented Ft Gordon network specialists from 2 to 1. ***Total Onboard = 87 (no change)*** **<<Current Updates Highlighted in Yellow>>**	MOD030

1 GENERAL

1.1 TASK ORDER TYPE: Hybrid (Firm Fixed Price / Cost Reimbursement / Time & Material)

1.2 BACKGROUND

MCIS's mission is to plan, program, acquire, implement and sustain peacetime information technology infrastructure, and to train personnel and provide support services for the MHS centrally managed products to improve and maintain the health of the MHS beneficiaries.

Military health care delivery is heavily dependent upon automated information systems (AISs) which rely on a robust network infrastructure to transport data within and between Medical Treatment Facilities (MTFs). Numerous medical and administrative systems use the network including: the Composite Health Care System (CHCS), AHLTA, Defense Medical Logistics Standard Support (DMLSS), Defense Blood Standard System (DBSS), Expense Assignment System (EAS) IV, as well as various office automation and electronic mail systems, suites, and clinical software add-ons. The protocols and technologies that are present on the MTF LANs and interconnecting WAN are described in **Attachment B.**

1.3 SCOPE

On behalf of Military Health System Cyberinfrastructure Services (MCiS), this awarded task order will provide network sustainment and deployment support services to the Military Health System (MHS) Medical Treatment Facilities (MTF) both inside and outside the continental United States (CONUS and OCONUS). This work includes functions such as network performance measurement and monitoring, assistance with network design and development, network measurement, customer service in the form of trouble tracking and troubleshooting at the Tier 0 level, onsite support for both contractor and Government support teams for escalated trouble tickets, as well as maintenance and sparing support. Such services will be provided in accordance with stated MHS and specific Medical Component priorities. Services shall also comply with existing and evolving technical architecture guidance from international, commercial, Department of Defense (DoD), and Health Affairs (HA) sources. These services will be provided in a centralized and decentralized mode. The on-site network specialists will be the primary 24/7 on-call decentralized points of contact within the MTFs. Additional support and guidance will be provided by regional (i.e. CONUS, Asia and Europe) network engineers, and the MCiS centralized infrastructure team. A complete list of sites and associated support staff is provided in **Attachment A**. The Government reserves the right to change this distribution to support mission criticality. A summary of the distribution of contractor staff is as follows:

A Regions

- Asia/Pacific
- Europe
- CONUS

B Number of network specialists

- Asia/Pacific - 11
- Europe - 6
- CONUS – 66

C Number of senior network engineers

- Asia/Pacific - 1
- Europe - 1
- CONUS – 2

D CONUS & OCONUS total task order requirement – 87 FTEs

1.4 OBJECTIVES

The objective of this tasking is for the contractor to provide network (i.e. local and wide area network) sustainment and deployment support services to the Military Health System (MHS) Medical Treatment Facilities (MTF), which includes hospitals, clinics, and other remote elements throughout CONUS and OCONUS locations. The Contractor shall, in the performance of this task order, be successful at coordinating and working with other vendors and Government agencies in resolving problems, gathering information, and/or making recommendations to the Government.

1.5 NON-PERSONAL SERVICES

This award identifies services that are strictly non-personal in nature.

1.6 SEVERABLE/NON-SEVERABLE SERVICES

This award identifies services that are Severable in nature.

1.7 INHERENTLY GOVERNMENTAL FUNCTIONS

This award has been reviewed and contains no services that are inherently governmental functions.

1.8 ACQUISITION FUNCTIONS CLOSELY ASSOCIATED WITH INHERENTLY GOVERNMENTAL FUNTIONS

Not applicable for this task.

1.9 ORGANIZATIONAL CONFLICT OF INTEREST CATEFORY

TRICARE Management Activity (TMA) has categorized all its non-purchased care requirements into three broad categories, as defined below, for purposes of identifying, avoiding or mitigating against Organizational Conflicts of Interest (OCIs) in accordance with FAR Subpart 9.5. These categories are defined as follows:

- **Category 1: TMA Internal Support:** Services which, by their very nature, give the Contractor access to extensive data about the contracts of all other TMA contractors.

- **Category 2: Program Management Support:** Services which assist TMA in planning and managing its activities and programs. This includes, for example: requirements analysis, acquisition support, budget planning and management, business process reengineering, program planning and execution support, and independent technical management support.

- **Category 3: Product Support:** Services or end items required to meet the mission requirements of TMA's non-purchased care activities and programs. This includes, for example: concept exploration and development; system design; system development and integration; COTS procurement and integration; internal development testing; deployment; installation; operations; and maintenance.

  Contractor participation in more than one of these areas may give rise to an unfair competitive advantage resulting from access to advance acquisition planning, source selection sensitive or proprietary information. Furthermore, contractor participation in more than one area may give rise to a real or apparent loss of contractor impartiality and objectivity where its advisory or planning assistance in one area potentially affects its present or future participation in another area.

  The purpose of this categorization is to accomplish the following three objectives: (1) to inform prospective Offerors that TMA presumes that award of a contract or order in the subject category

will give rise to real or apparent OCIs with respect to requirements in the other two categories; (2) to assist current contractors and prospective Offerors in developing their own business strategies regarding participation in TMA requirements and in identifying and, where possible, avoiding or mitigating against OCIs; and (3) to ensure that all current contractors and prospective Offerors are afforded the maximum practicable opportunity to compete for all TMA requirements consistent with the restrictions required under FAR Subpart 9.5 and sound business practices.

For purposes of identifying, avoiding and / or mitigating against OCIs, TMA will examine all its non-purchased care requirements and acquisitions regardless of the cognizant contracting activity or the type of contract vehicle used.

Each TMA non-purchased care solicitation will therefore be designated as falling within one of the three above defined categories. The work called for under this contract / order has been categorized by TMA as a non-purchased care task as:

Category 3: Product Support

TMA will administer this clause for purposes of award eligibility for each solicitation as follows:

An Offeror that has never provided support to TMA in any of the categories is eligible for award in any category without any further action required under this clause.

An Offeror that provides or has provided support to TMA in only one category of work and has never supported TMA in any other category (a single-category contractor) is eligible for award for any future requirement in that single category without further action under this clause.

2.0 STATEMENT OF WORK (SOW)

2.1 TASK MANAGEMENT

The Contractor shall provide sufficient management to ensure that this task is performed efficiently, accurately, on time, and in compliance with the requirements of this document. Specifically, the Contractor shall designate a single Task Manager to oversee this task and supervise staff assigned to this task. The Contractor shall ensure that a Monthly Progress Report is submitted in accordance with the requirements stated below.

2.1.1 Reporting

2.1.1.1 Weekly Vacancy Report – Deliverable 2

The Contractor shall provide a weekly report on the vacancies across all locations. The exact content of this report will be determined after contract award by the COR after collaboration with the Contractor.

2.1.1.2 Monthly Progress Report (MPR) – Deliverable 3

The Contractor shall prepare and deliver a Monthly Progress Report **(Deliverable 3)**, The MPR shall outline the following:

- progress (i.e. performance against schedule)
- status
- problems / issues encountered and related program impacts
- deliverables submitted
- schedule deviations
- current costs (i.e. firm-fixed-price payment, ODC/cost reimbursement, and any T&M hours/costs)
- significant events
- Customer Satisfaction – Report customer satisfaction rate semi-annually showing percentage of completed survey forms that qualitatively demonstrate customer satisfaction with MCIS's provision of service
- Trouble Ticket Resolution for Tier 0 (i.e not escalated to the Network Support Center) - Report percentage of calls resolved at the site

The MPR shall also include the following information by facility:

- Tier 0 Trouble Tickets opened, in progress, resolved and closed during the month
- LAN/WAN issues
- TCP/IP address changes
- Circuits in-use
- Circuits no longer in-use
- Circuits connected
- Circuits disconnected
- Circuit upgrades completed
- Updates to the network physical configuration topology diagrams
- LAN downtime
- WAN downtime
- Remote circuit uptime
- Router configuration changes
- Firewall/Security Suite configuration changes
- Miscellaneous monthly changes and other significant events
- Schedule of planned activities
- Activities completed to date
- Remaining activities, if applicable (plans vs. achievements)

- Lessons learned
- Risks and mitigation of risks
- Any government action needed
- Monthly Remedy tier 0 (initiated at site) ticket summary
- Document problems encountered and provide the resultant impacts.
- Other information requested by MCIS on a recurring or as requested basis.

2.1.2 Subcontractor Expenditures Report – Deliverable 4

If Subcontractors are used, the Contractor shall prepare and deliver a Subcontract Expenditures Report **(Deliverable 3)** that discloses actual subcontract expenditures by company name, business size standard (i.e. Woman Owned Business, Veteran Owned Business, etc.), and other socioeconomic programs (i.e. Indian Incentive Program, Historically Black Colleges and Universities and Minority Institutions, etc.).

2.1.3 Contract Work Breakdown Structure (CWBS)

Not applicable for this task order.

2.1.4 Integrated Master Schedule

Not applicable for this task order.

2.1.5 Earned Value Management (EVM)

Not applicable for this task order.

2.1.6 Transition Support

2.1.6.1 Incoming Transition Plan – Deliverable 5

In accordance with the solicitation, the Contractor shall provide a plan for 30 days incoming transition from contract to contract. The Contractor shall coordinate with the Government in planning and implementing a complete transition to the Contractor's support model. The Contractor shall collaborate with the Government to develop, deliver, and evolve an Incoming Transition Plan **(Deliverable 5)**. The Government will designate a transition period for the incoming Contractor to coordinate and work with the incumbent Contractor. This transition plan shall include, but is not limited to:

- Coordination with Government representatives,
- Review, evaluation and transition of current support services,
- Transition of historic data to new Contractor system,
- Government-approved training and certification process,
- Transfer of hardware warranties and software licenses (if applicable),
- Transfer of all necessary business and/or technical documentation,
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates and patches (if applicable),
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
- Distribution of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.,
- GFE inventory management assistance,
- Transfer and documentation of the receipt of Government Furnished Equipment (GFE) and Government Furnished Information (GFI) such as:
    - hardware/software
    - laptops/PCs
    - pagers/cell phones/calling cards
    - data/databases
    - Common Access Cards (CAC)
    - procedural manuals/guidelines
    - operating instructions

- historical data, e.g., memos, letters, correspondence, regulations, reports, documents and contract document library
- agreement documents, e.g., software licensing agreements

2.1.6.2 Outgoing Transition Plan (Optional – To be exercised as a unilateral right of the Government) – Deliverable 6

In accordance with the solicitation, the Contractor shall provide a plan **(Deliverable 6)** for 30 days outgoing transition for transitioning work from an active task order to a follow-on contract/order or Government entity. The Government will provide 30 days advanced notice to the Contractor prior to exercising this option. This transition may be to a Government entity, another Contractor or to the incumbent Contractor under a new contract/order. In accordance with the Government-approved plan, the Contractor shall assist the Government in planning and implementing a complete transition from this Contract and/or orders issued under this Contract to a successful provider. This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This transition plan shall include, but is not limited to:

- Coordination with Government representatives,
- Review, evaluation and transition of current support services,
- Transition of historic data to new Contractor system,
- Government-approved training and certification process,
- Transfer of hardware warranties and software licenses (if applicable),
- Transfer of all necessary business and/or technical documentation,
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates and patches (if applicable),
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes,
- Disposition of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.,
- Transfer and documentation of the delivery/return of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance.
- Applicable TMA debriefing and personnel out-processing procedures.
- Turn-in of all government keys, ID/access cards, and security codes.

2.1.7 Program Management Plan – Deliverable 7

The Contractor shall develop a Program Management Plan **(Deliverable 7)** that shall require Government approval. This plan shall be applied by the Contractor to manage, track and evaluate the Contract performance. The Program Management Plan shall consist of control policies and procedures in accordance with standard industry practices for project administration, execution and tracking.

The Program Management Plan shall include the following:

- Identification of milestones where Government information/activity is required and timeline dependencies for subsequent Contractor activities;
- An Integrated Master Management Plan (IMMP) describing the Contractor’s overall management approaches, policies and procedures including suggested project metrics; and,
- A detailed staffing plan.

The Program Management Plan shall be due thirty (30) calendar days after the award of the order.

2.1.8 Quality Control Plan – Deliverable 8

The Contractor shall prepare and adhere to a Quality Control Plan (**QCP - Deliverable 8)**. The QCP shall document how the Contractor will meet and comply with the quality standards established in this statement of work. At a minimum, the QCP must include a self-inspection plan, an internal staffing plan, and an outline of the procedures that the Contractor will use to maintain quality, timeliness, responsiveness, customer satisfaction, and any other requirements set forth in this solicitation.

2.1.9 Contingency Operations Plan – Deliverable 9

The Contractor shall develop and submit a Contingency Operations Plan to the Government. The Contingency Operations Plan shall be due ten (10) calendar days after the award of the order, and will be updated on a quarterly basis **(Deliverable 9)**. The Contingency Operations Plan shall document Contractor plans and procedures to maintain TMA support during an emergency. The Contingency Operations Plan shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- Planned temporary work locations or alternate facilities
- How the Contractor will communicate with TMA during emergencies
- A list of primary and alternate Contractor points of contact, each with primary and alternate:
- Telephone numbers
- E-mail addresses
- Procedures for protecting Government furnished equipment (if any)
- Procedures for safeguarding sensitive and/or classified Government information (if applicable)

2.1.10 Overseas Housing Allowance Validation/Revalidation – Deliverable 10

The Government will reimburse the Contractor for Overseas Housing Allowance paid to employees assigned to provide on-site support to an OCONUS MTF, not to exceed the rate provided by the Joint Travel Regulations (JTR). Within six months after task order award or employee assignment to an overseas location whichever is later, the Contractor shall submit, for each employee assigned to an overseas location, written estimates of costs, or actual costs if they are known. Annually thereafter by 1 April, the Contractor shall validate the need and amount of the Overseas Housing Allowance (OHA) by submitting the actual annual expenses of rent and utilities, supported by receipts or other satisfactory evidence, for each employee assigned to an overseas location. **Deliverable 10**

2.1.11 Operations During Emergency Situations

Individual contingency operation plans shall be activated immediately after determining that an emergency has occurred, shall be operational within twelve (12) hours of activation, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the contract is terminated, whichever comes first. In case of a life threatening emergency, the COR shall immediately make contact with the Contractor Task Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, the Contractor Task Manager shall promptly open an effective means of communication and verify:

- Key points of contact (Government and Contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential work products expected to continue production by priority

The Contractor Task Manager, in coordination with the COR, must make use of the resources and tools available to continue TMA contracted functions to the maximum extent possible under emergency circumstances. The Contractor must obtain approval from the COR and Contracting Officer prior to incurring costs over and above those allowed for under the terms of this contract. Regardless of contract

type, and of work location, Contractors performing work in support of authorized tasks within the scope of their contract shall charge those hours accurately in accordance with the terms of this contract.

2.1.12 Contractor Personnel Performance/Replacement

The contractor Task Manager and the three (3) Regional Senior Engineers shall be designated as Key Personnel. Substitutions of quoted Key Personnel shall not be allowed for a period of six (6) months after award. Any substitution or replacement of Key Personnel shall have qualifications equal to or greater than the individuals quoted. The Government reserves the right to pre-approve any replacement or substitution of Key Personnel.

Contractor personnel must submit necessary information to be issued a clearance prior to reporting for performance.

2.1.13 Contractor Training, Position Responsibilitie, and Qualifications

The Contractor is required to provide personnel trained in systems, equipment, and software identified in Appendix E 'Labor Category Responsibilities and Required Qualifications'. This Appendix outlines the position responsibilities and qualifications, including any necessary experience, education, and/or other skills required according to location assignment.

In the event the Government deploys new systems or equipment or implements new processes not identified in this Work Statement, the Contractor may request and the Government may approve training for Contractor employees on those new systems, equipment, software, or processes. Labor hours and instructional venues to support Government approved training may be charged against this contract.

2.1.14 Operations

When operating Government owned or leased equipment, the Contractor shall ensure proper security clearance, (ADP sensitivity I, II, III) full familiarity with operation processes and procedures, and full compliance with site specific regulations, processes and procedures. When performing system operations, the Contractor shall ensure that staff sign and adhere to a Non-disclosure Statement (Appendix C) and protect ALL patient and system information.

2.1.15 Geographic/Area Specific

2.1.15.1 CONUS

Follow local MTF guidance and policies.

2.1.15.2 Korea

Invited Contractor (IC) or Technical Representative (TR) Status under U.S. - Republic of Korea (ROK) shall be governed by the U.S.-ROK Status of Forces Agreement (SOFA) as implemented by USFK Reg 700-19 (http://8tharmy.korea.army.mil/g1_AG/Programs_Policy/UploadedFile/USFK/USFK_Reg_700-19_The_Invited_Contractor_and_Technical_Representative_Program.pdf).

2.1.15.3 Europe

Invited Contractor or Technical Representative Status under NATO Status of Forces Agreement (SOFA)

- North Atlantic Treaty Organization (NATO) Status of Forces Agreement (SOFA), Google NATO SOFA

2.1.15.3.1 Germany: Use *Army Europe (AE) Regulation 715-9*, referenced below and in Section 7.1, for policies, procedures and guidance relating to current and future employment of contractor personnel in Germany.

- www.eur.army.mil/g1/content/CPD/.../SA_Overview-Germany.pptx

2.1.15.3.2 Italy: Use *"Tri-Component Directive for Italy on Personal Property, Rationed Goods, Motor Vehicles and Drivers' Licenses, Civilian Component and Technical Representative Status";*, referenced in

Section 7.1, for policies, procedures and guidance relating to current and future employment of contractor personnel in Germany.

"Tri-Component Directive for Italy on Personal Property, Rationed Goods, Motor Vehicles and Drivers' Licenses, Civilian Component and Technical Representative Status"

- http://www.eur.army.mil/g1/content/CPD/docs/docper/tricomponent_directive.pdf , current version is dated February 20, 2004.

2.1.15.3.3 Spain: Use Annex Six, *"Contracting for Works and Services*" within the *"Agreement of Defense Cooperation between the USA and the Kingdom of Spain*," referenced in Section 7.1, for policies, procedures and guidance relating to current and future employment of contractor personnel in Spain.

- Annex Six, "*Contracting for Works and Services*" within the "*Agreement of Defense Cooperation between the USA and the Kingdom of Spain*," http://madrid.usembassy.gov/about-us/odc/agreement.html, current version is dated April, 10 2002

2.1.16 ADP Sensitivity Designation Report – Deliverable 13

provide a report each quarter, or as requested, to include any required Trustworthiness Status letters for employees in a pending status for over 1 year.

2.2 SPECIFIC TASKS

2.2.1 Network Support

The Contractor shall provide on-site network (i.e. local and wide area network) sustainment and deployment support services to the Military Health System (MHS) Medical Treatment Facilities (MTF), which includes hospitals, clinics, and other remote elements throughout CONUS and OCONUS locations, as described in Section titled 'SCOPE'. The Contractor shall support the overall network infrastructure at an MTF and respond to, detect, report, record, diagnose and resolve the occurrence of network faults as well as measure network performance and connectivity on a ongoing basis. The Contractor shall serve as an on-site resource for site coordination, troubleshooting, problem resolution, local inventory interfaces with MTF staff, and shall provide customer service and guidance to the various site staff within the MTFs. The Contractor may be required to provide support to the MTF in the following areas:

- Install, relocate, configure, modify and test routers, hubs, switches, wireless access points and associated controllers, and terminal servers.
- Create, maintain and manage Virtual Local Area Networks (VLANs).
- Install, test, terminate and maintain cable. (Such installation will provide no warranty of installed cable or drops. All material and equipment required will be provided by the Government).
- Troubleshoot wiring problems.
- Certify wiring drops.
- Troubleshoot serial communication lines.
- Operate and maintain Network Management Systems (NMS).
- Manage network operating systems (NOS).
- Support diagnostics and configuration connectivity of MHS site/service specific servers, such as DBSS, CHCS, AHLTA, DMLSS, operating systems, office automation, etc.
- Maintain MHS site telecommunications systems.
- Assist with the establishment and implementation of network policies, procedures and standards to include network security.
- Support the MTF management staff with briefings and updates on network issues.
- Complete MCiS furnished Sparing & Maintenance hardware inventories.
- Manage security firewalls/Virtual Private Network (VPN) devices.

- Collect Performance Measurement information.
- Assist with MCiS Infrastructure deployments and technical hardware refresh initiatives. Submit a schedule indicating the projected date(s) when each piece of equipment will be installed (**Deliverable 11**).
- Participate in long-range MHS infrastructure planning and technical architecture
- Develop, plan and maintain documentation necessary for operations in support of LAN to WAN connectivity.
- Define and recommend minimum standards, as applies to network operations, access to the Internet and its impact on overall network resourcing and operations.
- Oversee the integration of network hardware and software platforms for WAN/LAN connected systems and medical AISs at MTFs, clinics, etc. as directed by the COR.
- Coordinate telecommunications actions with all applicable agencies and organizations as required.
- Address user concerns with the LAN/WAN service provider and alert users to routine maintenance impacting circuits.
- Provide network related advice to DoD medical information systems personnel.
- Share information with the contractor's senior engineering staff such as lessons learned and issues requiring higher level technical or management involvement for resolution

2.2.2 Network Development

Additionally, the Contractor shall perform infrastructure analysis, integration and support of new technologies and products and communicate with external agencies for site-related activities and implementation actions and provide Technical Reports, Evaluations and Recommendations (see **Deliverable 3**) to include recommendations on technical solutions for regional upgrades, or network changes, such as:

- Evaluate and recommend new and evolving networking technologies.
- Evaluate vendor products.
- Assess data, voice, and video network requirements.
- Propose implementation strategies.
- Propose enhancements or design changes to improve the efficiency of the networks.

2.2.3 Network Management

- The Contractor shall provide a Semi-Annual Inventory Report (**Deliverable 12**) that reflects the MCiS equipment inventory. The report shall include a description of the equipment, model number, serial number, software version, location and any other pertinent information and utilize steps as well as guidelines set forth within the MCiS Inventory Standard Operating Procedure (SOP). In addition to the above stated, the contractor shall employ the use of the current system of record pertaining to Asset Management.

- The Contractor shall conduct/attend any walk-through and/or meeting where contractor maintained systems are discussed. The Contractor shall participate in Integrated Product Teams (IPT) as directed by the Government.

2.2.4 System Support

In the process of providing network support, the Contractor shall be required to interface with MHS systems in troubleshooting network issues and in deliniating between system and network problems. This compentency requires a basic knowledge of MHS system infrastructure and application systems,

and applicable hardware and software configuration, operation and support skills. The Contractor shall apply any necessary software maintenance processes at, or equivalent to, the SEI CMM Level II, or higher.

2.2.4.1 System Support (Sembach, Germany) – General systems administration support is required for specific Government systems. See description of required support in **Attachment E** "Systems and Network Specialist (Sembach, Germany).

3.0 INSPECTION AND ACCEPTANCE

The Contracting Officer's Representative (COR) for the Task Order is a Government official who has been delegated specific technical, functional and oversight responsibilities for this task order. The COR is designated in the COR appointment letter, issued by the Contracting Officer, and is responsible for inspection and acceptance of all services, incoming shipments, documents, and services.

3.1 Acceptance Criteria

Certification by the Government of satisfactory services provided is contingent upon the Contractor performing in accordance with the performance standards contained in the Performance Requirements Summary Matrix (Section 6.8.2) and all terms and conditions of this order, including all modifications.

3.2 Contractor Payment Processing

The Contractor is responsible for properly preparing and forwarding to the appropriate Government official in a timely fashion, the invoice and receiving report for payment. When the ITSS – Receipt and Acceptance application is able to be used, it is the preferred method of submission.

4.0 DELIVERABLES

4.1 Delivery Address

All deliverables shall be submitted to the COR, and the follow email address:

TIMPODeliverables@tma.osd.mil

4.2 Method of Delivery

Electronic copies shall be delivered using Microsoft Office suite of tools (for example, MS WORD, MS EXCEL, MS POWERPOINT, MS PROJECT, or MS ACCESS format), unless otherwise specified by the COR. Electronic submission shall be made via email, unless otherwise agreed to by the COR.

4.3 Shipping

The Contractor shall use the U.S. Postal Service standard delivery for delivery of materials, equipment, or required hardcopy documents. The COR must approve all exceptions to this requirement.

4.4 Government Acceptance Period

The COR will have ten (10) workdays to review draft deliverables and make comments. The Contractor shall have five (5) workdays to make corrections. Upon receipt of the final deliverables, the COR will have two (2) workdays for final review prior to acceptance or providing documented reasons for non-acceptance. Should the Government fail to complete the review within the review period the deliverable will become acceptable by default, unless prior to the expiration of the ten (10) work days the Government notifies the Contractor in writing to the contrary. The final submission should be deemed approved if the Government has not rejected it in thirty (30) calendar days.

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted quote. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have five (5) workdays to correct the rejected deliverable and return it per delivery instructions.

4.5 Delivery Schedule Abbreviations

The following abbreviations are used in the delivery/deliverable schedule:

Abbreviation	Definition
AM	Acquisition Manager
COR	Contracting Officer's Representative for the Task order

CS	Contract Specialist
DA	Days after
DACA	Days after contract award (award of this order)
DAEOM	Days after the end of the month
Days	Calendar Days unless otherwise specified
DID	Data Item Description
E	Electronic Copy
H	Hard Copy
NLT	Not Later Than
PWS Ref	Performance Work Statement Reference (paragraph number)

4.6 Deliverable / Delivery Schedule

A summary of deliverables follows. Copies are to be provided to the Government officials indicated in electronic file (E), and/or hard copy (H).

Item	PWS Ref	Title	Dist.	E	H	Initial	Subsequent
Deliverable 1	Attachment C	Non-Disclosure Agreement	COR AM		1 1	Signed statements are due, from each employee assigned, *prior to* performing *ANY* work on this task.	
Deliverable 2	2.1.1.1	Weekly Vacancy Report	COR AM	1 1		Delivery of first report as determined by Contractor Task Manager and COR	Weekly – specific day, as defined by COR
Deliverable 3	2.1.1.2	Monthly Progress Report	COR AM	1 1		NLT 45 DACA	NLT 15th of each month
Deliverable 4	2.1.2	Subcontract Expenditures Report	CS AM COR	1 1 1	1 1	NLT 90 DACA	Quarterly thereafter. A final submission reflecting all expenditures on this order is due within 5 days of completion of the order.
Deliverable 5	2.1.6.a	Transition Plan – Incoming Transition	COR	1		NLT 1 DACA	N/A
Deliverable 6	2.1.6.b	Transition Plan – Outgoing Transition	COR	1		NLT 90 DACA	Updated as required, but NLT 3 DA incumbent is notified of non-award
Deliverable 7	2.1.7	Program Management Plan	COR AM	1 1		NLT 30 DACA	Updated as required
Deliverable 8	2.1.8	Quality Control Plan	COR	1		NLT 30 DACA	Updated as required
Deliverable 9	2.1.9	Contingency Operations Plan	COR	1		NLT 10 DACA	Updated quarterly

Item	PWS Ref	Title	Dist.	E	H	Initial	Subsequent
Deliverable 10	2.1.10	Overseas Housing Allowance Reimbursement Validation/Revalidation Report	COR AM	1 1		Within 6 Months of contract award	Within 6 months of employee assignment and annually by 1 April
Deliverable 11	2.2.1	Schedule of Equipment Refresh	COR AM	1		NLT 7 calendar days after receipt of equipment	
Deliverable 12	2.2.3	Semi-annual Inventory of equipment	COR	1			NLT 15 February and 15 August of each year
Deliverable 13	2.1.16	**ADP Sensitivity Designation Report**	COR	1		Delivery of first report as determined by Contractor Task Manager and COR	Quarterly – specific day, as defined by COR

5.0 CONTRACT ADMINISTRATION DATA

Period of performance shall be for a base period of 12 months and 4 option periods of 12 months each.

5.1 Place of Performance

The Contractor shall perform primary activity at the Government facilities, as indicated above, unless otherwise stated or required by Government.

The Government will provide access to Government controlled facilities, equipment, and materials for daily business use of staff called for under this order. This shall include office space, desk, telephone, chair, computer, shared printer, and requisite consumable materials.

The Contractor will be provided keys or codes for access to the Government facility. These keys and codes shall be controlled, tracked, and protected. Upon termination of the period of performance, all keys and/or access badges to the Government facility shall be turned in to the COR.

5.2 Other Direct Costs (ODCs)

Only contractors with adequate accounting or purchasing systems will be allowed to procure and invoice ODCs. All ODC purchases require prior authorization by the COR. ODCs shall be billed on a cost reimbursable basis. Costs are defined as the purchase price of materials or service plus General and Administrative charges (G&A) or material and handling charges (M&H). G&A or M&H charges received by the Contractor are subject to periodic Government conducted DCAA audits and to adjustment as a result of the final contract closeout audit conducted by DCAA. All ODCs shall be fully supported in compliance with all competition requirements of the FAR, specifically Part 31. All ODCs shall be reported as stated in the Procurement of Hardware, Software, Equipment and Materials Section 2.2.3.1, as well as the Monthly Progress Report Section 2.1.2.2.

The following ODC's lists a description with an estimated annual amount:

Description	**Quantity**
Overseas Housing Allowance	***$ 650,000***
OCONUS Cost of Living Allowance	***$ 172,080***
OCONUS Dependent Education Expense	***$ 153,775***
Materials	***$100,000***
Relocation	***$150,000***
Travel	***$250,000***

5.2.1 Travel

Arrangements for and costs of all travel, transportation, meals, lodging, and incidentals are the responsibility of the Contractor. Travel costs shall be incurred and billed in accordance with the Joint Travel Regulations (JTR). Costs for these expenses will be reviewed, certified and approved by the COR. All travel and transportation shall utilize commercial sources and carriers. The Government will not pay for business class or first-class travel.

5.2.2 Travel Outside of the U.S.

This order includes activity that may require Contractor travel to destinations outside of the United States. The Contractor shall ensure that assigned participants allow sufficient lead-time to obtain valid passports, country clearances, and immunizations to support project activities. All travel outside of the U.S. required under this tasking shall be in accordance with the Joint Travel Regulations (JTR).

5.2.3 Optional Items

The Government reserves the unilateral right to exercise the items, Optional Items X002 and X003 which will be invoked through award of task order modifications issued by the Contracting Officer. Options may be invoked, in whole or in part, at the discretion of the Government. The Contractor will be provided 30-days from time of option exercise to begin performance of optional work.

5.2.4 Points of Contact

DHA HIT IOD Contracting Officer's Representative (COR) - Primary
Jeffery W. Collins
Function Chief, Core Infrastructure Services
DHA Network Operations Center
Network Affairs Section
Health Information Technology Directorate
E-mail: jeffery.w.collins14.civ@mail.mil
Tel: 210.295.3014
Mobil: 210.501.8743

DHA HIT IOD Contracting Officer's Representative (COR) - Secondary
Beau Kiser
Defense Health Agency, Health Information Technology
Infrastructure & Operations Division
Operations and Sustainment Branch Chief,
Network Affairs Section
E-mail: samuel.h.kiser.civ@mail.mil
Tel: 210-338-3331

DHA HIT IOD Contracting Officer's Representative (COR) - Europe
Ronald Locker
E-mail: ronald.e.locker.civ@mail.mil
Tel: 011-49-170-219-8528

MCiS Contracting Officer's Representative (COR) – Asia/Pacific
Lawrence Owens
E-mail: lawrence.r.owens.civ@mail.mil

GSA Contracting Officer (CO)
Alex Garcia
GSA-FAS, Mid-Atlantic Region
100 S Independence Mall West
3rd Floor
Philadelphia, PA 19106
E-mail: alexander.garcia@gsa.gov
Tel: 215-446-5868

GSA Contracting Officer's Technical Representative (COTR)
Allen Cardwell
100 S Independence Mall West
3rd Floor
Philadelphia, PA 19106
E-mail: allen.cardwell@gsa.gov
Tel: 215-446-5831

6.0 OTHER TERMS, CONDITIONS, AND PROVISIONS

6.1 Non-Disclosure / Non-Use Agreement – Deliverable 1

The Contractor shall ensure that the Non-Disclosure Statement (**Attachment C - Deliverable 1**) is signed by all staff assigned to or performing on this Task order before performing any work, including all subcontractors and consultants. The Non-Disclosure / Non-Use statement shall be cosigned by a corporate official (Contractor Task Manager or higher). The Contractor shall also ensure that all staff understand and adhere to the terms of the non-disclosure statement, protecting the procurement sensitive information of the Government and the proprietary information of other Contractors. Assignment of staff who have not executed this statement or failure to adhere to this statement shall constitute default on the part of the Contractor.

6.2 Information Assurance

MHS System/Application Security Certification and Accreditation (C&A) Support

The contractor shall support the DIACAP certification and accreditation of assigned MHS systems/applications to support the secure operations and maintenance of MHS environments, including processing:

- Controlled Unclassified Information (CUI) data.
- Privacy Act data.
- Classified data (within the confines of a separate, SIPRNet-connected, hosting facility area).

The C&A support of the contractor shall include:

- Conducting and completing required Facility, Automated Information System, and Network Infrastructure security checklists as well as other security checklists identified by the COR.
- Developing required DIACAP security documentation.
- Supporting security surveys and site visits.
- Responding to security personnel questions and inquires.
- Support implementation of required physical, electronic, and procedural safeguards and facility enhancements (including changes, relocations, downtime coordination, and other activities needed to meet facility security safeguards).
- Developing and maintaining any required facility security accreditation documentation and other inputs directed by the COR.

6.3 Enterprise Architecture (EA)

6.3.1 Internet Protocol version 6 (IPv6)

The Contractor shall provide COTS solutions that are IPv6 capable. An IPv6 capable system or product shall be capable of receiving, processing, transmitting and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to that of IPv4. Specific criteria to be deemed IPv6 capable are:

- Conformance to the DoD Information Technology Standards Repository (DISR) developed DoD IPv6 Standards Profile. Systems being developed, procured or acquired shall comply with the Global Information Grid Architecture and DISR standard IPv6 Capable definition. An IPv6 Capable system must meet the IPv6 base requirements defined in the “DoD IPv6 Standards Profile v1.0” dated June 1, 2006 available from the DISR.

- Maintenance of interoperability with IPv4. Systems being developed, procured or acquired shall maintain interoperability with IPv4 systems/capabilities. Systems should implement IPv4/IPv6dual-stack and should also be built to determine which protocol layer to use depending

on the destination host it is attempting to communicate with or establish a socket with. If either protocol is possible, systems should employ IPv6.

- Evidence of a migration path and commitment to upgrade all applications and product features to IPv6 by June 2008.

- Availability of contractor/vendor IPv6 technical support for system development, implementation and management.

  DoD IPv6 security guidelines, standards, and solutions shall be utilized and adhered to when available. Currently, DoD IPv6 Information Assurance (IA) guidance is available from the DoD IPv6 Transition Office (DITO).

6.4 Protection of Information

6.4.1 Dissemination of Information/Publishing

There shall be no dissemination or publication, except within and between the Contractor and any subcontractors or specified Integrated Product/Process Team (IPT) members who have a need to know, of information developed under this order or contained in the reports to be furnished pursuant to this order without prior written approval of the TMA COR or the Contracting Officer. TMA approval for publication will require provisions which protect the intellectual property and patent rights of both TMA and the Contractor.

6.4.2 Contractor Employees

- **Contractor Identification**
  The Contractor shall ensure that Contractor personnel identify themselves as Contractors when attending meetings, answering Government telephones, providing any type of written correspondence, or working in situations where their actions could be construed as official Government acts.

- **Attendance at Meetings**
  Contractor personnel may be required to attend meetings or otherwise communicate with Government and/or other contract representatives to meet the requirements of this order. Contractor personnel shall make their Contractor status known during introductions.

- **Use of Military Rank by Contractor Personnel**
  Contractor personnel, while performing in a Contractor capacity, are prohibited from using their retired or reserve component military rank or title in all written or verbal communications associated with the contracts under which they provide services.

6.4.3 Personally Identifiable Information (PII) and Protected Health Information (PHI)

The Contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all Government data. The Contractor shall also ensure the confidentiality, integrity, and availability of Government data in compliance with all applicable laws and regulations, including data breach reporting and response requirements, in accordance with DFAR Subpart 224.1 (Protection of Individual Privacy), which incorporates by reference DoDD 5400.11, “DoD Privacy Program,” May 8, 2007, and DoD 5400.11-R, “DoD Privacy Program,” May 14, 2007. The contractor shall also comply with federal laws relating to freedom of information and records management.

Health Insurance Portability and Accountability Act (HIPAA)

The Contractor shall comply with all requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191), as implemented by the HIPAA Privacy and Security Rules codified at 45 C.F.R. Parts 160 and 164, and as further implemented within the Military Health System

(MHS) by DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003, and DoD 8580.02-R, “DoD Health Information Security Regulation, July 12, 2007. The Contractor shall also comply with all applicable HIPAA-related rules and regulations as they are published and as further defined by later-occurring Government requirements and DoD guidance, including current and forthcoming DoD guidance implementing applicable amendments under the American Recovery and Reinvestment Act of 2009 (ARRA). Any rules and regulations that are published, and/or requirements that are defined after the award date of this contract, and that require expenditure of additional Contractor resources for compliance, may be considered “changes” and will be subject to the “changes” clause under the contract.

Breach Response

DoD 5400.11-R, “DoD Privacy Program,” May 14, 2007, defines a breach as the “actual or possible loss of control, unauthorized disclosure, or unauthorized access of personal information where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected.” Within one hour of discovery, the breach must be reported to the US Computer Emergency Readiness Team (US CERT) at https://forms.us-cert.gov/report/ and to the TMA Privacy Office at PrivacyOfficerMail@tma.osd.mil.

The Contractor shall adhere to the reporting and response requirements set forth in the Office of the Secretary of Defense (OSD) Memorandum 1504-07, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” June 5, 2009; DoD 5400.11-R, and applicable TMA Privacy Office guidance, including current and forthcoming DoD guidance on ARRA breach notification requirements, available at: http://www.tricare.mil/tma/privacy/breach.aspx.

Systems of Records

In order to meet the requirements of 5 U.S.C. 552a, the Privacy Act of 1974, and its implementation within the Military Health System (MHS) under DoD 5400.11-R, “ DoD Privacy Program,” May 14, 2007, Contractors must identify to the Contracting Officer Representative (COR) systems of records that are maintained or operated for TMA where records of personally identifiable information (PII) collected from individuals are maintained and specifically retrieved using a personal identifier. Upon identification of such systems to the COR, and prior to the lawful operation of such systems, Contractors must coordinate with the TMA Privacy Office at SORmail@tma.osd.mil to complete systems of records notices (SORNs) for submission and publication in the *Federal Register* as coordinated by the Defense Privacy Office, and as required by DoD 5400.11-R.

Following proper SORN publication and Government confirmation of Contractor authority to operate the applicable system(s), Contractors must also comply with the additional systems of records and SORN guidance, in coordination with the TMA Privacy Office, regarding periodic system review, amendments, alterations, or deletions set forth by DoD 5400.11-R, Office of Management and Budget (OMB) Memorandum 99-05, Attachment B, and OMB Circular A-130.

Privacy Impact Assessment (PIA)

The Contractor shall provide for the completion of a Privacy Impact Assessment (PIA) for any applicable systems that collect, maintain, use or disseminate personally identifiable information (PII) or protected health information (PHI) about members of the public, federal personnel, contractors, or in some cases foreign nationals.

To begin the PIA process, Contractors are responsible for the completion of the PIA Determination Checklist. This Checklist provides basic system information to the TMA Privacy Office and ensures that the appropriate decision concerning PIA requirements is made. The Checklist can be downloaded from http://www.tricare.mil/tma/privacy/downloads/2010513/TMAPIADeterminationChecklist.pdf.

Contractors are responsible for the employment of practices that satisfy the requirements and regulations of: Section 208 of E-Government (E-Gov) Act of 2002, (Pub. L. 107-347); DoDI 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009; and, Office of Management and Budget (OMB) Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," September 26, 2003. When completing a PIA, the Contractor is responsible for using the DoD-approved PIA Template, DD Form 2930, available at http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd2930.pdf.

Completed PIA Determination Checklists and DD Form 2930s will be sent to the TMA Privacy Office at piamail@tma.osd.mil.

Data Use Agreement (DUA)

A Data Use Agreement (DUA) is currently used to request and control the disclosure, use, storage and/or destruction of MHS data that is owned and/or managed by TMA to ensure that applicable privacy and security requirements are followed. In addition, research requests for MHS data that include protected health information (PHI) must be reviewed for HIPAA compliance by the TMA Privacy Board.

Under DoD 6025.18-R, "DoD Health Information Privacy Program," January 24, 2003, reasonable steps must be taken to implement appropriate procedural, administrative, technical and physical safeguards to prevent the unauthorized use and/or disclosure of any personally identifiable information (PII) or PHI. Likewise, all uses, disclosures, and destruction of PII and PHI data are generally subject to DoD 5400.11-R, "DoD Privacy Program," May 14, 2007, as well as DoDI 8500.2, "Information Assurance (IA) Implementation," Feb. 6, 2003, and DoD 8580.02-R, "DoD Health Information Security Regulation," July 12, 2007.

To begin the DUA request process, the contractor should choose the applicable request template at http://www.tricare.mil/tma/privacy/Templates.aspx, or should contact DUAmail@tma.osd.mil. After receiving DUA approval, anyone needing access to information system applications or data sources must contact the responsible system program office. DUAs are active for one year, or until the end of the current option year, whichever comes first. If the DUA will not be renewed, the TMA contractor must provide a Certificate of Data Destruction (CDD) to the TMA Privacy Office.

Privacy Act and HIPAA Training

The Contractor shall ensure that all staff including subcontractors and consultants comply with the training requirements of the Privacy Act of 1974 (5 U.S.C. 552a) and Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Pub. L. 104-191). The training requirements are mandated by OSD Memorandum 15041-07, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information": DoD 6025.18-R, "DoD Health Information Privacy Regulation", January 24, 2003; and the TMA Workforce Training Policy Memorandum, dated May 28, 2008, on the subject, "Workforce Training Policy Pursuant to the Department of Defense Privacy Act Regulations and the Department of Defense Health Insurance Portability and Accountability Act Privacy and Security Regulations".

The Contractor shall ensure that the annual Privacy Act and HIPAA training is completed by all staff assigned to or performing on this Task Order, including subcontractors and consultants. All required Privacy Act and HIPAA training will be conducted online through Military Health System Learn (MHS Learn) at https://mhslearn.csd.disa.mil or the current TMA learning management system (LMS) in place to deliver training to meet the above requirements. The Contractor shall ensure all employees and subcontractors supply a certificate of Privacy Act and HIPAA training completion to the Contracting Officer Representative (COR) within 30 days of being assigned to the Task Order and on an annual basis based on the trainee's birth month thereafter.

Records Management

When creating and maintaining official government records, the Contractor shall comply with all federal requirements established by 44 United States Code (USC), 41 USC, 36 Code of Federal Regulations (CFR), Department of Defense (DOD) Administrative Instruction No. 15 (DOD AI-15), "Records Management, Administrative Procedures and Records Disposition Schedules," and Chapter 2 of the TRICARE Operations Manual.

Freedom of Information Act (FOIA) Office
TRICARE Freedom of Information (FOIA) procedures require a written request under the Act to be addressed to the FOIA Officer, TMA, 16401 East Centretech Parkway, Aurora, Colorado 80011-9066. The request shall describe the desired record as completely as possible to facilitate its retrieval from files and to reduce search fees which may be borne by the requestor. No more than ten working days shall elapse after a request has been received by the Freedom of Information Officer before notification is sent that the request has been granted or denied. The administrative time limit for responding to FOIA requests does not begin until the request is received by TMA.

In response to requests received by contractors for the release of information, unclassified information, documents and forms which were previously provided to the public as part of routine services shall continue to be made available in accordance with previously established criteria. All other requests from the public for release of TRICARE records and, specifically, all requests that reference the Freedom of Information Act shall be immediately forwarded to TMA, ATTENTION: Freedom of Information Officer, for appropriate action. **Direct contact, including interim replies, between TRICARE contractors and such requestors is not authorized**. The contractor shall process requests by individuals for access to records about themselves under the Privacy Act procedures when those procedures are more advantageous to the requestor.

6.4.4 Protection of Human Subjects and Adherence to Ethical Standards in Department of Defense (DoD)-Supported Research

DFARS 252.235-7004-PROTECTION OF HUMAN SUBJECTS (JUL 2009)

(a) *Definitions*. As used in this clause—
(1) "Assurance of compliance" means a written assurance that an institution will comply with requirements of 32 CFR Part 219, as well as the terms of the assurance, which the Human Research Protection Official determines to be appropriate for the research supported by the Department of Defense (DoD) component (32 CFR 219.103).
(2) "Human Research Protection Official (HRPO)" means the individual designated by the head of the applicable DoD component and identified in the component's Human Research Protection Management Plan as the official who is responsible for the oversight and execution of the requirements of this clause, although some DoD components may use a different title for this position.
(3) "Human subject" means a living individual about whom an investigator (whether professional or student) conducting research obtains data through intervention or interaction with the individual, or identifiable private information (32 CFR 219.102(f)). For example, this could include the use of human organs, tissue, and body fluids from individually identifiable living human subjects as well as graphic, written, or recorded information derived from individually identifiable living human subjects.
(4) "Institution" means any public or private entity or agency (32 CFR 219.102(b)).
(5) "Institutional Review Board (IRB)" means a board established for the purposes expressed in 32 CFR Part 219 (32 CFR 219.102(g)).
(6) "IRB approval" means the determination of the IRB that the research has been reviewed and may be conducted at an institution within the constraints set forth by the IRB and by other institutional and Federal requirements (32 CFR 219.102(h)).
(7) "Research" means a systematic investigation, including research, development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of 32 CFR Part 219, whether or not they are conducted or supported under a program that is considered research for other purposes. For example, some demonstration and service programs may include research activities (32 CFR 219.102(d)).

(b) The Contractor shall oversee the execution of the research to ensure compliance with this clause. The Contractor shall comply fully with 32 CFR Part 219 and DoD Directive 3216.02, applicable DoD component policies, 10 U.S.C. 980, and, when applicable, Food and Drug Administration policies and regulations.
(c) The Contractor shall not commence performance of research involving human subjects that is covered under 32 CFR Part 219 or that meets exemption criteria under 32 CFR 219.101(b), or expend funding on such effort, until and unless the conditions of either the following paragraph (c)(1) or (c)(2) have been met:
(1) The Contractor furnishes to the HRPO, with a copy to the Contracting Officer, an assurance of compliance and IRB approval and receives notification from the Contracting Officer that the HRPO has approved the assurance as appropriate for the research under the Statement of Work and also that the HRPO has reviewed the protocol and accepted the IRB approval for compliance with the DoD component policies. The Contractor may furnish evidence of an existing assurance of compliance for acceptance by the HRPO, if an appropriate assurance has been approved in connection with previous research. The Contractor shall notify the Contracting Officer immediately of any suspensions or terminations of the assurance.
(2) The Contractor furnishes to the HRPO, with a copy to the Contracting Officer, a determination that the human research quoted meets exemption criteria in 32 CFR 219.101(b) and receives written notification from the Contracting Officer that the exemption is determined acceptable. The determination shall include citation of the exemption category under 32 CFR 219.101(b) and a rationale statement. In the event of a disagreement regarding the Contractor's furnished exemption determination, the HRPO retains final judgment on what research activities or classes of research are covered or are exempt under the contract.
(d) DoD staff, consultants, and advisory groups may independently review and inspect the Contractor's research and research procedures involving human subjects and, based on such findings, DoD may prohibit research that presents unacceptable hazards or otherwise fails to comply with DoD procedures.
(e) Failure of the Contractor to comply with the requirements of this clause will result in the issuance of a stop-work order under Federal Acquisition Regulation clause 52.242-15 to immediately suspend, in whole or in part, work and further payment under this contract, or will result in other issuance of suspension of work and further payment for as long as determined necessary at the discretion of the Contracting Officer.
(f) The Contractor shall include the substance of this clause, including this paragraph (f), in all subcontracts that may include research involving human subjects in accordance with 32 CFR Part 219, DoD Directive 3216.02, and 10 U.S.C. 980, including research that meets exemption criteria under 32 CFR 219.101(b). This clause does not apply to subcontracts that involve only the use of cadaver materials
.

6.4.5 Business Associates

Introduction

In accordance with DoD 6025.18-R "Department of Defense Health Information Privacy Regulation," January 24, 2003, the Contractor meets the definition of Business Associate. Therefore, a Business Associate Agreement is required to comply with both the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations. This clause serves as that agreement whereby the Contractor agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as defined in this clause, and in DoD 6025.18-R and DoD 8580.02-R, as amended. Additional requirements will be addressed when implemented.

(a) **Definitions**. As used in this clause generally refer to the Code of Federal Regulations (CFR) definition unless a more specific provision exists in DoD 6025.18-R or DoD 8580.02-R.

Individual has the same meaning as the term "individual" in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

Protected Health Information has the same meaning as the term "protected health information" in 45 CFR 160.103, limited to the information created or received by the Contractor from or on behalf of the Government pursuant to the Contract.

Electronic Protected Health Information has the same meaning as the term "electronic protected health information" in 45 CFR 160.103.

Required by Law has the same meaning as the term "required by law" in 45 CFR 164.103.

Secretary means the Secretary of the Department of Health and Human Services or his/her designee.

Security Rule means the Health Insurance Reform: Security Standards at 45 CFR part 160, 162 and part 164, subpart C.

Terms used, but not otherwise defined, in this Clause shall have the same meaning as those terms in 45 CFR 160.103, 160.502, 164.103, 164.304, and 164.501.

(b) The Contractor shall not use or further disclose Protected Health Information other than as permitted or required by the Contract or as Required by Law.

(c) The Contractor shall use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Contract.

(d) The Contractor agrees to use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits in the execution of this Contract.

(e) The Contractor shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Contractor of a use or disclosure of Protected Health Information by the Contractor in violation of the requirements of this Clause. These mitigation actions will include as a minimum those listed in the TMA Breach Notification Standard Operating Procedure (SOP), which is available at: http://www.tricare.mil/tma/privacy/breach.aspx.

(f) The Contractor shall report to the Government any security incident involving protected health information of which it becomes aware.

(g) The Contractor shall report to the Government any use or disclosure of the Protected Health Information not provided for by this Contract of which the Contractor becomes aware.

(h) The Contractor shall ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by the Contractor, on behalf of the Government, agrees to the same restrictions and conditions that apply through this Contract to the Contractor with respect to such information.

(i) The Contractor shall ensure that any agent, including a subcontractor, to whom it provides electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.

(j) The Contractor shall provide access, at the request of the Government, and in the time and manner reasonably designated by the Government to Protected Health Information in a Designated

Record Set, to the Government or, as directed by the Government, to an Individual in order to meet the requirements under 45 CFR 164.524.

(k) The Contractor shall make any amendment(s) to Protected Health Information in a Designated Record Set that the Government directs or agrees to pursuant to 45 CFR 164.526 at the request of the Government, and in the time and manner reasonably designated by the Government.

(l) The Contractor shall make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by the Contractor, on behalf of the Government, available to the Government, or at the request of the Government to the Secretary, in a time and manner reasonably designated by the Government or the Secretary, for purposes of the Secretary determining the Government's compliance with the Privacy Rule.

(m) The Contractor shall document such disclosures of Protected Health Information and information related to such disclosures as would be required for the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

(n) The Contractor shall provide to the Government or an Individual, in time and manner reasonably designated by the Government, information collected in accordance with this Clause of the Contract, to permit the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

General Use and Disclosure Provisions

Except as otherwise limited in this Clause, the Contractor may use or disclose Protected Health Information on behalf of, or to provide services to, the Government for treatment, payment, or healthcare operations purposes, in accordance with the specific use and disclosure provisions below, if such use or disclosure of Protected Health Information would not violate the HIPAA Privacy Rule, the HIPAA Security Rule, DoD 6025.18-R or DoD 8580.02-R if done by the Government.

Specific Use and Disclosure Provisions

(a) Except as otherwise limited in this Clause, the Contractor may use Protected Health Information for the proper management and administration of the Contractor or to carry out the legal responsibilities of the Contractor.

(b) Except as otherwise limited in this Clause, the Contractor may disclose Protected Health Information for the proper management and administration of the Contractor, provided that disclosures are required by law, or the Contractor obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Contractor of any instances of which it is aware in which the confidentiality of the information has been breached.

(c) Except as otherwise limited in this Clause, the Contractor may use Protected Health Information to provide Data Aggregation services to the Government as permitted by 45 CFR 164.504(e)(2)(i)(B).

(d) Contractor may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

Obligations of the Government

Provisions for the Government to Inform the Contractor of Privacy Practices and Restrictions

(a) The Government shall provide the Contractor with the notice of privacy practices that the Government produces in accordance with 45 CFR 164.520.

(b) The Government shall provide the Contractor with any changes in, or revocation of, permission by Individual to use or disclose Protected Health
Information, if such changes affect the Contractor's permitted or required uses and disclosures.

(c) The Government shall notify the Contractor of any restriction to the use or disclosure of Protected Health Information that the Government has agreed to in accordance with 45 CFR 164.522.

Permissible Requests by the Government

The Government shall not request the Contractor to use or disclose
Protected Health Information in any manner that would not be permissible under the HIPAA Privacy Rule, the HIPAA Security Rule, or any applicable Government regulations (including without limitation, DoD 6025.18-R and DoD 8580.02-R) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Contractor as otherwise permitted by this clause.

Termination

(a) Termination. A breach by the Contractor of this clause, may subject the Contractor to termination under any applicable default or termination provision of this Contract.

(b) Effect of Termination.

(1) If this contract has records management requirements, the records subject to the Clause should be handled in accordance with the records management requirements. If this contract does not have records management requirements, the records should be handled in accordance with paragraphs (2) and (3) below

(2) If this contract does not have records management requirements, except as provided in paragraph (3) of this section, upon termination of this Contract, for any reason, the Contractor shall return or destroy all Protected Health Information received from the Government, or created or received by the Contractor on behalf of the Government. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of the Contractor. The Contractor shall retain no copies of the Protected Health Information.

(3) If this contract does not have records management provisions and the Contractor determines that returning or destroying the Protected Health Information is infeasible, the Contractor shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the Contractor that return or destruction of Protected Health Information is infeasible, the Contractor shall extend the protections of this Contract to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as the Contractor maintains such Protected Health Information.

Miscellaneous

(a) Regulatory References. A reference in this Clause to a section in DoD 6025.18-R, DoD 8580.02-R, Privacy Rule or Security Rule means the section currently in effect or as amended, and for which compliance is required.

(b) Survival. The respective rights and obligations of Business Associate under the "Effect of Termination" provision of this Clause shall survive the termination of this Contract.

(c) Interpretation. Any ambiguity in this Clause shall be resolved in favor of a meaning that permits the Government to comply with DoD 6025.18-R, DoD 8580.02-R, the HIPAA Privacy Rule or the HIPAA Security Rule.

6.4.6 Public Key Infrastructure Authentication and Encryption.
Contractors shall follow the DoD standards, policies, and procedures related to the use of Public Key Infrastructure (PKI) certificates and biometrics for positive authentication including authentication to DoD private web servers or applications. Where interoperable PKI is required for the exchange of unclassified information, including the encryption of e-mail containing sensitive information, between DoD and its Contractors, industry partners shall obtain all necessary certificates if they are not eligible for a DoD Common Access Card. (refer to http://iase.disa.mil/pki/eca/ and http://www.cac.mil/)

6.5 Access Requirements

6.5.1 Contractor access to HA/TMA Network/DoD Systems
The Contractor will require access to the HA/TMA Network/DoD Systems to perform work under this task.

6.5.2 Contractor access to classified information
The Sr. Engineers will require access to classified data to perform this task. Necessary DD254 will be provided after the award.

6.5.3 Contractor access to Planning Programming, Budgeting, and Execution (PPBE) Documents and Data
Not Applicable for this Task

6.6 Development
Not applicable for this task.

6.7 Data Rights
The Government will retain rights to all data produced in the course of developing, deploying, training, using and supporting TMA or other federal agencies that utilize this order.

6.8 Quality Assurance
The Government shall review Monthly Progress Reports and shall attend regular task performance review meetings with the Contractor to survey quality of products and services.

6.8.1 Quality Assurance Surveillance Plan (QASP)
The Government intends to utilize a Quality Assurance Surveillance Plan (QASP) to monitor the quality of the Contractor's performance. The oversight provided for in the order and in the QASP will help to ensure that service levels reach and maintain the required levels throughout the contract term. Further, the QASP provides the COR with a proactive way to avoid unacceptable or deficient performance, and provides verifiable input for the required Past Performance Information Assessments. The QASP will be finalized immediately following award and a copy provided to the Contractor after award. The QASP is a living document and may be updated by the Government as necessary.

6.8.2 Performance Requirements Summary Matrix
By monitoring the Contractor, the COR will determine whether the performance levels set forth in the order have been attained. Performance standards are specified in the following Performance Requirements Summary Matrix in the Standard and Acceptable Quality Level columns.

Task	Indicator	Standard	Acceptable Quality Level	Method of Surveillance	Incentive
1. Complete reports	Completed in a timely manner	Reports submitted as required in 4.5 & 4.6	Not more than 5% late	Monthly check of submission logs	Positive Past Performance Evaluation
2. Provide problem diagnosis and resolution	Problems are resolved	Responses are accurate, current and tailored to the individual needs of the caller and to the MTF	Receive no more than three valid complaints about service during the month	Customer Complaints	Positive Past Performance Evaluation
3. Maintain network equipment	Equipment is available for MTF operations	Equipment failures, non-availability or maintenance shall not interfere with MTF operations	Equipment failures, non-availability or maintenance do not interfere with MTF operations for more than 72 hours during a month	Customer Complaints; Random Inspections	Positive Past Performance Evaluation
4. Dispose of excess equipment	No excess equipment is stored at MTF.	Equipment that is at the end of its lifecycle or is otherwise excess or unusable will be turned in or disposed per Government direction in a timely manner	Excess equipment will be turned in or disposed of within 7 workdays of identification	Random inspection, valid receipts from Tobyhanna or other disposal facilities	Positive Past Performance Evaluation
5. Satisfy Customer	MTF management is satisfied with support provided	Semi-annual Customer Satisfaction Surveys report satisfactory or better performance	Survey results of not less than average of 3 on 5-point Likert Scale for 12-month period	Reported to TM with Monthly Progress Report	Positive Past Performance Evaluation

Task	Indicator	Standard	Acceptable Quality Level	Method of Surveillance	Incentive
6. Perform inventory	Inventory report is accurate and submitted for all sites	Semi-annual inventory report accurately reflects all existing network infrastructure equipment and contains the information required by 2.2.3	Inventory contains all required information, is 95% accurate, includes each site with no more than two sites missing deadline by no more than 15 days	Random inspections	Positive Past Performance Evaluation

6.8.3 Performance Evaluation Process

The Contractor Performance Assessment Reporting System (CPARS) has been adopted by TMA to electronically capture assessment data and manage the evaluation process. CPARS is used to assesses a Contractor's performance and provide a record, both positive and negative, on a given contract during a specific period of time. The CPARS process is designed with a series of checks and balances to facilitate the objective and consistent evaluation of Contractor performance. Both Government and Contractor program management perspectives are captured on the CPAR form and together make a complete CPAR. Once the Assessing Official completes the quoted assessment for the period of performance, the CPAR is released to the appropriate Government Contractor Representative for their review and comments. User ID and Password will be provided to the designated Government Contractor Representative upon issuance of a task order. The Contractor has 30 days after the Government's evaluation is completed to comment on the evaluation. The Government Contractor Representative must either concur or non-concur to each CPAR. If the Contractor concurs with the quoted assessment and the Reviewing Official does not wish to see the CPAR, the Assessing Official may close out the CPAR. Otherwise, they must forward the CPAR to the Reviewing Official for them to review, enter comments if appropriate, and close out. The Reviewing Official may at their option direct the Assessing Official to forward every CPAR to them for review.

6.9 Government Furnished Equipment (GFE)/ Information (GFI)/Property (GFP)

The Government may provide the equipment/information/property shown in the attached listing of Government Furnished Equipment/Information/Property.

The Contractor shall maintain a detailed inventory accounting system for Government Furnished Equipment/Material or Contractor-Acquired-Government Owned Property (CAP). The inventory accounting system must specify, as a minimum: product description (make, model), Government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if CAP), and contract/order number under which the equipment is being used. The Contractor shall either: a) attach an update inventory report to each Monthly Progress Report, or b) certify that the inventory has been updated and is available for Government review. In either case the Contractor's inventory listing must be available for Government review within one business day of COR request.

6.10 Section 508 Requirement

The Contractor shall comply with Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d). Specifically, the procurement, development, maintenance, or integration of electronic and information

technology (EIT) under this contract must comply with the applicable accessibility standards issued by the Architectural and Transportation Barriers Compliance Board at CFR part 1194.

6.11 Other Special Considerations

6.12 Invoicing

BILLING/INVOICING

***Billing and Payment**. Billing and payment shall be accomplished in accordance with instructions below. The firm fixed price portion of the contract shall be based on **1/12th of the total firm fixed price for labor each month**, with separate line items for any reimbursable travel.*

The Contractor shall provide original invoices to the address shown on Block 24 of the GSA Form 300 award document. A concurrent copy of each invoice shall be sent to the Client Representative (CR).

Invoices (January/2010)

The Period of Performance (POP) for each invoice *shall* be for one calendar month. The contractor *shall* submit only one invoice per month per order/contract. The appropriate GSA office will receive the invoice by the twenty-fifth calendar day of the month after either:

(1) The end of the invoiced month (*for services*) or
(2) The end of the month in which the products *(commodities)* or deliverables (fixed-priced services) were delivered and accepted by the Government.

For Labor Hour and Time and Material orders/contracts each invoice *shall* show, the skill level category, the hours worked per skill level, the rate per skill level and the extended amount for that invoice period. It *shall* also show the total cumulative hours worked (inclusive of the current invoice period) per skill level, the hourly rate per skill level, the total cost per skill level, the total travel costs incurred and invoiced, and the total of any other costs incurred and invoiced, *as well as* the grand total of all costs incurred and invoiced.

For Labor Hour and Time and Material orders/contracts each invoice *shall clearly indicate* both the current invoice's monthly "burn rate" and the total average monthly "burn rate".

The contractor *shall submit* all required documentation (unless exempted by the contract or order) as follows:

For Travel: Submit the traveler's name, dates of travel, location of travel, and dollar amount of travel.

For ODCs: Submit a description of the ODC, quantity, unit price and total price of each ODC.

Note: The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travel and ODCs.

Posting Acceptance Documents: Invoices shall initially be submitted monthly through GSA's electronic Web-Based Order Processing System, currently ITSS, to allow the client and GSA COTR to electronically accept and certify services received by the CR. Included with the invoice will be all back-up documentation required such as, but not limited to, travel authorizations and training authorizations (including invoices for such).

Receiving Agency's Acceptance: The receiving agency has the following options in accepting and certifying services;

a. Electronically: The client agency may accept and certify services electronically via GSA's electronic Web-Based Order Processing System, currently ITSS, by accepting the Acceptance Document generated by the contractor. Electronic acceptance of the invoice by the CR is considered concurrence and acceptance of services. ***NOTE: The Government's preference is that receiving agency's acceptance is conducted electronically.***
b. On Paper Copy: The client agency may accept and certify services by providing written acceptance with the signature of the authorized client representative and the date of acceptance.

Electronic and/or written acceptance of the invoice by the CR is considered concurrence and acceptance of services. Regardless, of the method of acceptance the contractor shall seek acceptance and electronically post the acceptance document in GSA's electronic Web-based Order Processing System, currently ITSS. (Written acceptances will be posted as an attachment along with any other supporting documentation.) After acceptance of the invoice by the CR, the Contractor shall submit a proper invoice to GSA Finance not later than five (5) workdays after acceptance by the Government of the product, service, and/or cost item.

Note: The acceptance of the authorized agency customer representative is REQUIRED prior to the approval of payment for any invoiced submitted. Although this acceptance may occur in two ways, electronically or in paper copy, at least shall be obtained prior to the approval of payment. In order to expedite payment, it is *strongly recommended* that the contractor continue to include the receiving agency's WRITTEN acceptance of all the services or products delivered, with signature of the authorized agency customer representative and the date of acceptance, as part of the submission documentation.

Note: If *any* invoice is received without the required documentation and, (A) the customer's *signed* written acceptance OR (B) the customer's electronic acceptance, the invoice *shall* be rejected in whole or in part as determined by the Government.

Posting Invoice Documents: Contractors shall submit invoices to GSA Finance for payment, after acceptance has been processed in GSA's electronic Web-Based Order Processing System, currently ITSS. The contractor has the option of posting the invoice on GSA's Ft. Worth web site, www.finance.gsa.gov/defaultexternal.asp or mail to the address shown on BLOCK 24 of the GSA FORM 300. ***NOTE: Only use one method of submission, web site or regular U.S. mail, but not both.***

U.S. Mailing Address:

General Services Administration

Financial Operations and Disbursement Branch (BCEB)

PO BOX 219434

KANSAS CITY, MO 64121-9434

Content of Invoice: The contractor's invoice will be submitted monthly for work performed the prior month. The contractor may invoice only for the hours, travel and unique services ordered by GSA and actually used in direct support of the client representative's project. The invoice shall be submitted on official letterhead and shall include the following information at a minimum.

1. GSA Task Order Number
2. Task Order ACT Number
3. Remittance Address
4. Period of Performance for Billing Period
5. Point of Contact and Phone Number
6. Invoice Amount
7. Skill Level Name and Associated Skill Level Number
8. Actual Hours Worked During the Billing Period
9. Travel Itemized by Individual and Trip (if applicable)
10. Training Itemized by Individual and Purpose (if applicable)
11. Support Items Itemized by Specific Item and Amount (if applicable)

Final Invoice: Invoices for final payment must be so identified and submitted within 60 days from task completion and no further charges are to be billed. A copy of the written acceptance of task completion must be attached to final invoices. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

The Government reserves the right to require certification by a GSA COTR before payment is processed, *if necessary.*

Close-out Procedures.

General: The contractor shall submit a final invoice within sixty (60) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

6.13 Clauses

The following FAR clauses are hereby incorporated by reference:

- FAR 52.204-9 - Personal Identity Verification of Contractor Personnel (Sep 2007)
- FAR 52.217-8 - Option to Extend Services (Nov 1999) – and/or –
- FAR 52.217-9 - Option to Extend the Term of the Contract (Mar 2000)
- FAR 52.224-2 - Privacy Act Notification" (Apr 1984)
- FAR 52.224-2 - Privacy Act (Apr 1984)
- FAR 52.237-3 - Continuity of Services (Jan 1991)
- FAR 52.245-1 - Government Property (Aug 2010)
- Clause regarding FAR 9.5 Organizational Conflict of Interest
- FAR 52.228-3 Workers Compensation Insurance (Defense Base Act)(April 1984)

THE FOLLOWING CLAUSES ARE HEREBY INCORPORATE IN ENTIRETY:

CONTRACTOR MANPOWER REPORTING

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Defense Health Agency (DHA - UIC DDAAFC) via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address: http://www.ecmra.mil/

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), WHICH RUNS October 1 through September 30. While inputs may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year, beginning with 2013. Contractors may direct questions to the help desk at: http://www.ecmra.mil/"

5352.223-9001 HEALTH AND SAFETY ON GOVERNMENT INSTALLATIONS (JUN 1997)

(a) In performing work under this contract on a Government installation, the contractor shall:

(1) Comply with the specific health and safety requirements established by this contract;

(2) Comply with the health and safety rules of the Government installation that concern related activities not directly addressed in this contract;

(3) Take all reasonable steps and precautions to prevent accidents and preserve the health and safety of contractor and Government personnel performing or in any way coming in contact with the performance of this contract; and

(4) Take such additional immediate precautions as the contracting officer may reasonably require for health and safety purposes.

(b) The contracting officer may, by written order, direct Air Force Occupational Safety and Health Standards (AFOSH) and/or health/safety standards as may be required in the performance of this contract and any adjustments resulting from such direction will be in accordance with the Changes clause of this contract.

(c) Any violation of these health and safety rules and requirements, unless promptly corrected as directed by the contracting officer, shall be grounds for termination of this contract in accordance with the Default clause of this contract.

(END OF CLAUSE)

5352.225-9102 Submission of Offers for Contracts to be Performed in the Federal Republic of Germany

SUBMISSION OF OFFERS FOR CONTRACTS TO BE PERFORMED IN THE FEDERAL REPUBLIC OF GERMANY (USAFE) (SEP 2003)

This contract may require the performance of services in the Federal Republic of Germany (Germany).

(a) In accordance with the Exchange of Notes (Dated 27 Mar 98) in implementation of Articles 72 and 73 of the German Supplementary Agreement (SA) to North Atlantic Treaty Organization (NATO) Status of Forces Agreement (SOFA), Non-German citizens of a NATO member country who perform services on Government contracts shall not start work in Germany without meeting one of the following criteria:

(1) Technical Expert Status accreditation (TESA)

(2) Troop Care Status accreditation (TCSA)
(3) Analytical Support Status accreditation (ASSA)
(4) Military Exigency (ME) via TESA or ASSA
(5) TESA/ASSA TDY
(6) Exemption from German work permit ("fax back")
(7) German work permit or compliance with European Union member nation exchange laws and regulations

(8) Certificates of limited tax liability and a German work permit

(b) Contractor employees who receive the status identified in items (a)(1) through (a)(5) in the above paragraph are granted SOFA Status. The process for contractors to obtain SOFA status is a two-part process. First, the contract must be approved as meeting the requirements set forth in Articles 72 and/or 73 of the German SA to the NATO SOFA. Next, individual contractor employees may be submitted for approval against an approved contract. Contractors who meet the criteria for one of the items at (a)(1) through (a)(5) above are considered to be, and are treated as, a part of the civilian component. Thus, they are entitled to Individual Logistics Support from the US Forces and will not be subject to German income tax so long as the reason for the individual's presence in Germany is "solely due to their temporary presence there" because of their employment. Logistics Support for contractors performing under TESA/ASSA TDY will be determined by the USAFE SOFA coordinator on a case-by-case basis.

(c) The contractor shall comply with the requirements and procedures identified by the Department of Defense Contractor Personnel Office (DOCPER). The direction and forms are available at the following internet site http://www.per.hqusareur.army.mil/content/CPD/docper.html (After entering the site, click on DOCPER). This site also contains information and forms for item (a)(6) above, "fax back" procedures.

(d) The contractor shall ensure that identification cards and/or other logistics support documents pertinent to, or peculiar to, SOFA status are turned over to the issuing office upon termination or transfer of individual contractor employees. Within three days of completion, the contractor shall provide written proof to the contracting officer that all identification cards and other logistics support documents have been returned to the government.

(e) If the contractor's employees will be performing in the Federal Republic of Germany under the conditions identified in paragraphs (a)(6) through (a)(8) of this clause, DOCPER is not involved in the process.

(f) The contracting officer [ ] does [ ] does not require the contractor to identify and submit a list of positions for which TESA, TCSA, or ASSA is sought and the applicable position description for each of the positions with the contractor's proposal/bid. The contractor shall only submit positions that meet the criteria set forth in Articles 72 and 73. In the event that any or all positions identified in the contractor's proposal are disapproved after contract award, the contract price shall not be subject to adjustment.

(End of Provision)

5352.225-9103 Contracts to be Performed in the Federal Republic of Germany

CONTRACTS TO BE PERFORMED IN THE FEDERAL REPUBLIC OF GERMANY (USAFE) (SEP 2003)

(a) In accordance with the exchange of notes (dated 27 Mar 98) implementing the Provisions of Articles 72 and 73 of the German Supplementary Agreement (SA) to the North Atlantic Treaty Organization (NATO) Status of Forces Agreement (SOFA), non-German citizens of a NATO member country who perform services on US Government contracts shall not start work in Germany without meeting one of the following criteria:

(1) Technical Expert Status accreditation (TESA)
(2) Troop Care Status accreditation (TCSA)
(3) Analytical Support Status accreditation (ASSA)
(4) Military Exigency (ME) via TESA or ASSA
(5) TESA/ASSA TDY
(6) Exemption from German work permit ("fax back")
(7) German work permit or compliance with European Union member nation exchange laws and regulations
(8) Certificates of limited tax liability and a German work permit

(b)In order to request status under paragraph (a)(1) through (a)(5) above, immediately after contract award, the contractor shall submit to the contracting officer in accordance with USAFEFARS 5325.10110 a Contract Notification package. The contractor shall submit Technical Expert Status (TES)/ Troop Care Status (TCS)/ Analytical Support Status (ASS) application packages for any employees for which TES/TCS/ASS accreditation is sought within three business days of the individual being hired.

(c) The packages/applications cited in paragraph (b) above shall be submitted through the contracting officer (or the contracting officer's appointed representative) to DOCPER. DOCPER's contact information is available at the DOCPER Internet site http://www.per.hqusareur.army.mil/content/CPD/docper.html

(d) A 10-week temporary TES or ASS may be granted by the US Government for purposes of Military Exigency (ME). ME is granted for time sensitive, mission critical positions for the purpose of permitting individual contract employees, who upon initial review of the application appear to meet the requirements of TES or ASS, to begin working in Germany prior to TES/ASS accreditation.

(e) The contractor shall notify the contracting officer within three days in writing of TES/TCS/ASS accreditation duties or when a TES/TCS/ASS employee is no longer assigned to the position for which TES/TCS/ASS accreditation was granted.

(1) The contractor shall ensure that identification cards and/or other logistics support documents pertinent to, or peculiar to, TES/TCS/ASS are turned over to the issuing office upon termination or transfer of individual contractor employees. Within three days of completion, the contractor shall provide written proof to the contracting officer that all identification cards and other logistics support documents have been returned to the government.

(f) The contractor shall allow German government authorities to visit the contractor's work areas for the purpose of verifying the status of positions and personnel as Technical Expert (TE)/Troop Care (TC)/Analytical Support (AS) employees. Such visits will not excuse the contractor from performance under this contract or result in increased costs to the Government.

(g) The contract price shall not be subject to an economic adjustment with regard to TES/TCS/ASS in the event that

(1) the contract and any or all positions identified in the contractor's proposal are disapproved for

TES/TCS/ASS accreditation; or

(2) any or all positions submitted for TES/TCS/ASS consideration during the life of the contract are disapproved for TES/TCS/ASS accreditation; or

(3) any or all contractor employees are denied TES/TCS/ASS; or

(4) TES/TCS/ASS accreditation is rescinded during the life of the contract.

(h) If the contractor's employees will be performing in the Federal Republic of Germany under the conditions identified in paragraphs (a)(6) through (a)(8) of this clause, DOCPER is not involved in the process.

(End of Clause)

225.7401 Contracts requiring performance or delivery in a foreign country.

(a) If an acquisition requires performance of work in a foreign country by contractor personnel other than host country personnel, or delivery of items to a Unified Combatant Command designated operational area, follow the procedures at PGI 225.7401(a)

(http://www.acq.osd.mil/dpap/dars/pgi/pgi_htm/PGI225_74.htm).

(b) For work performed in Germany, eligibility for logistics support or base privileges of contractor employees is governed by U.S.-German bilateral agreements. Follow the procedures in Army in Europe Regulation 715-9, available at http://www.per.hqusareur.army.mil/content/CPD/docper.html.

(c) For work performed in Japan or Korea, see PGI 225.7401(c) for information on bilateral agreements and policy relating to contractor employees in Japan or Korea.

252.225-7020 Trade Agreements Certificate.

TRADE AGREEMENTS CERTIFICATE (JAN 2005)

(a) Definitions. "Designated country end product," "non-designated country end product," "qualifying country end product," and "U.S.-made end product" have the meanings given in the Trade Agreements clause of this solicitation.

(b) Evaluation. The Government—

(1) Will evaluate offers in accordance with the policies and procedures of Part 225 of the Defense Federal Acquisition Regulation Supplement; and

(2) Will consider only offers of end products that are U.S.-made, qualifying country, or designated country end products unless—

(i) There are no offers of such end products;

(ii) The offers of such end products are insufficient to fulfill the Government's requirements; or

(iii) A national interest waiver has been granted.

(c) Certification and identification of country of origin.

(1) For all line items subject to the Trade Agreements clause of this solicitation, the offeror certifies that each end product to be delivered under this contract, except those listed in paragraph (c)(2) of this provision, is a U.S.-made, qualifying country, or designated country end product.

(2) The following supplies are other non-designated country end products:

(Line Item Number)	(Country of Origin)
N/A	N/A

(End of provision)

252.225-7021 Trade Agreements.

As prescribed in 225.1101(6), use the following clause:

TRADE AGREEMENTS (MAR 2007)

(a) Definitions. As used in this clause

(1) “Caribbean Basin country end product”

(i) Means an article that

(A) Is wholly the growth, product, or manufacture of a Caribbean Basin country; or

(B) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a Caribbean Basin country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services (except transportation services) incidental to its supply, provided that the value of those incidental services does not exceed the value of the product itself; and

(ii) Excludes products, other than petroleum and any product derived from petroleum, that are not granted duty-free treatment under the Caribbean Basin Economic Recovery Act (19 U.S.C. 2703(b)). These exclusions presently consist of□

(A) Textiles, apparel articles, footwear, handbags, luggage, flat goods, work gloves, leather wearing apparel, and handloomed, handmade, or folklore articles that are not granted duty-free status in the Harmonized Tariff Schedule of the United States (HTSUS);

(B) Tuna, prepared or preserved in any manner in airtight containers; and

(C) Watches and watch parts (including cases, bracelets, and straps) of whatever type, including, but not limited to, mechanical, quartz digital, or quartz analog, if such watches or watch parts contain any material that is the product of any country to which the HTSUS column 2 rates of duty (HTSUS General Note 3(b)) apply.

(2) “Component” means an article, material, or supply incorporated directly into an end product.

(3) “Designated country” means—

(i) A World Trade Organization Government Procurement Agreement (WTO GPA) country (Aruba, Austria, Belgium, Bulgaria, Canada, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea (Republic of), Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Singapore, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, or the United Kingdom);

(ii) A Free Trade Agreement country (Australia, Bahrain, Canada, Chile, Dominican Republic, El Salvador, Guatemala, Honduras, Mexico, Morocco, Nicaragua, or Singapore);

(iii) A least developed country (Afghanistan, Angola, Bangladesh, Benin, Bhutan, Burkina Faso, Burundi, Cambodia, Cape Verde, Central African Republic, Chad, Comoros, Democratic Republic of Congo, Djibouti, East Timor, Equatorial Guinea, Eritrea, Ethiopia, Gambia, Guinea, Guinea-Bissau, Haiti, Kiribati, Laos, Lesotho, Madagascar, Malawi, Maldives, Mali, Mauritania, Mozambique, Nepal, Niger, Rwanda, Samoa, Sao Tome and Principe, Senegal, Sierra Leone, Solomon Islands, Somalia, Tanzania, Togo, Tuvalu, Uganda, Vanuatu, Yemen, or Zambia); or

(iv) A Caribbean Basin country (Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, British Virgin Islands, Costa Rica, Dominica, Grenada, Guyana, Haiti, Jamaica, Montserrat, Netherlands Antilles, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, or Trinidad and Tobago).

(4) “Designated country end product” means a WTO GPA country end product, a Free Trade Agreement country end product, a least developed country end product, or a Caribbean Basin country end product.

(5) “End product” means those articles, materials, and supplies to be acquired under this contract for public use.

(6) “Free Trade Agreement country end product” means an article that□

(i) Is wholly the growth, product, or manufacture of a Free Trade Agreement country; or

(ii) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a Free Trade Agreement country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services (except transportation services) incidental to its supply, provided that the value of those incidental services does not exceed the value of the product itself.

(7) “Least developed country end product” means an article that—

(i) Is wholly the growth, product, or manufacture of a least developed country; or

(ii) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a least developed country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services (except transportation services) incidental to its supply, provided that the value of those incidental services does not exceed the value of the product itself.

(8) “Nondesignated country end product” means any end product that is not a U.S.-made end product or a designated country end product.

(9) “Qualifying country” means any country set forth in subsection 225.872-1 of the Defense Federal Acquisition Regulation Supplement.

(10) “Qualifying country end product” means□

(i) An unmanufactured end product mined or produced in a qualifying country; or

(ii) An end product manufactured in a qualifying country if the cost of the following types of components exceeds 50 percent of the cost of all its components:

(A) Components mined, produced, or manufactured in a qualifying country.

(B) Components mined, produced, or manufactured in the United States.

(C) Components of foreign origin of a class or kind for which the Government has determined that sufficient and reasonably available commercial quantities of a satisfactory quality are not mined, produced, or manufactured in the United States.

(11) “United States” means the 50 States, the District of Columbia, and outlying areas.

(12) “U.S.-made end product” means an article that□

(i) Is mined, produced, or manufactured in the United States; or

(ii) Is substantially transformed in the United States into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed.

(13) “WTO GPA country end product” means an article that□

(i) Is wholly the growth, product, or manufacture of a WTO GPA country; or

(ii) In the case of an article that consists in whole or in part of materials from another country, has been substantially transformed in a WTO GPA country into a new and different article of commerce with a name, character, or use distinct from that of the article or articles from which it was transformed. The term refers to a product offered for purchase under a supply contract, but for purposes of calculating the value of the end product includes services (except transportation services) incidental to its supply, provided that the value of those incidental services does not exceed the value of the product itself.

(b) Unless otherwise specified, this clause applies to all items in the Schedule.

(c) The Contractor shall deliver under this contract only U.S.-made, qualifying country, or designated country end products unless—

(1) In its offer, the Contractor specified delivery of other nondesignated country end products in the Trade Agreements Certificate provision of the solicitation; and

(2)(i) Offers of U.S.-made, qualifying country, or designated country end products from responsive, responsible offerors are either not received or are insufficient to fill the Government’s requirements; or

(ii) A national interest waiver has been granted.

(d) The contract price does not include duty for end products or components for which the Contractor will claim duty-free entry.

(e) The HTSUS is available on the Internet at http://www.usitc.gov/tata/hts/bychapter/index.htm. The following sections of the HTSUS provide information regarding duty-free status of articles specified in paragraph (a)(2)(ii)(A) of this clause:

(1) General Note 3(c), Products Eligible for Special Tariff Treatment.

(2) General Note 17, Products of Countries Designated as Beneficiary Countries Under the United States--Caribbean Basin Trade Partnership Act of 2000.

(3) Section XXII, Chapter 98, Subchapter II, Articles Exported and Returned, Advanced or Improved Abroad, U.S. Note 7(b).

(4) Section XXII, Chapter 98, Subchapter XX, Goods Eligible for Special Tariff Benefits Under the United States--Caribbean Basin Trade Partnership Act.

(End of clause)

252.229-7002 Customs Exemptions Germany

CUSTOMS EXEMPTIONS Germany (JUN 1997)

Imported products required for the direct benefit of the United States Forces are authorized to be acquired duty-free by the Contractor in accordance with the provisions of the Agreement Between the United States of America and Germany Concerning Tax Relief to be Accorded by Germany to United States Expenditures in the Interest of Common Defense.

(End of clause)

Subpart 9903.202 -- Disclosure Requirements.

9903.202-1 -- General Requirements.

(a) A Disclosure Statement is a written description of a contractor's cost accounting practices and procedures. The submission of a new or revised Disclosure Statement is not required for any non-CAS-covered contract or from any small business concern.

(b) Completed Disclosure Statements are required in the following circumstances:

(1) Any business unit that is selected to receive a CAS-covered contract or subcontract of $50 million or more shall submit a Disclosure Statement before award.

(2) Any company which, together with its segments, received net awards of negotiated prime contracts and subcontracts subject to CAS totaling $50 million or more in its most recent cost accounting period, must submit a Disclosure Statement before award of its first CAS-covered contract in the immediately following cost accounting period. However, if the first CAS-covered contract is received within 90 days of the start of the cost accounting period, the contractor is not required to file until the end of 90 days.

(c) When a Disclosure Statement is required, a separate Disclosure Statement must be submitted for each segment whose costs included in the total price of any CAS-covered contract or subcontract exceed $650,000, unless

(i) The contract or subcontract is of the type or value exempted by 9903.201–1 or

(ii) In the most recently completed cost accounting period the segment's CAS-covered awards are less than 30 percent of total segment sales for the period and less than $10 million.

(d) Each corporate or other home office that allocates costs to one or more disclosing segments performing CAS-covered contracts must submit a Part VIII of the Disclosure Statement.

(e) Foreign contractors and subcontractors who are required to submit a Disclosure Statement may, in lieu of filing a Form No CASB–DS–1, make disclosure by using a disclosure form prescribed by an agency of its Government, provided that the Cost Accounting Standards Board determines that the information disclosed by that means will satisfy the objectives of Public Law 100–679. The use of alternative forms has been approved for the contractors of the following countries:

(1) Canada.

(2) Federal Republic of Germany

(3) United Kingdom.

(f) Educational institutions—disclosure requirements.

(1) Educational institutions receiving contracts subject to the CAS specified in part 9905 are subject to the requirements of 9903.202, except that completed Disclosure Statements are required in the following circumstances.

(2) Basic requirement. For CAS-covered contracts placed on or after January 1, 1996, completed Disclosure Statements are required as follows:

(i) Any business unit of an educational institution that is selected to receive a CAS-covered contract or subcontract in excess of $650,000 and is part of a college or university location listed in Exhibit A of Office of Management and Budget (OMB) Circular A–21 shall submit a Disclosure Statement before award.

(ii) Any business unit that is selected to receive a CAS-covered contract or subcontract of $25 million or more shall submit a Disclosure Statement before award.

(iii) Any educational institution which, together with its segments, received net awards of negotiated prime contracts and subcontracts subject to CAS totaling $25 million or more in its most recent cost accounting period, of which, at least one award exceeded $1 million, must submit a Disclosure Statement before award of its first CAS-covered contract in the immediately following cost accounting period. However, if the first CAS-covered contract is received within 90 days of the start of the cost accounting period, the institution is not required to file until the end of 90 days.

(3) Transition period requirement. For CAS-covered contracts placed on or before December 31, 1995, completed Disclosure Statements are required as follows:

(i) For business units that are selected to receive a CAS-covered contract or subcontract in excess of $650,000 and are part of the first 20 college or university locations (i.e., numbers 1 through 20) listed in Exhibit A of OMB Circular A–21, Disclosure Statements shall be submitted within six months after the date of contract award.

(ii) For business units that are selected to receive a CAS-covered contract or subcontract in excess of $650,000 and are part of a college or university location that is listed as one of the institutions numbered 21 through 50, in Exhibit A of OMB Circular A–21, Disclosure Statements shall be submitted during the six month period ending twelve months after the date of contract award.

(iii) For business units that are selected to receive a CAS-covered contract or subcontract in excess of $650,000 and are part of a college or university location that is listed as one of the institutions numbered 51 through 99, in Exhibit A of OMB Circular A–21, Disclosure Statements shall be submitted during the six month period ending eighteen months after the date of contract award.

(iv) For any other business unit that is selected to receive a CAS-covered contract or subcontract of $25 million or more, a Disclosure Statement shall be submitted within six months after the date of contract award.

(4) Transition period due dates. The educational institution and cognizant Federal agency should establish a specific due date within the periods prescribed in 9903.202–1(f)(3) when a Disclosure Statement is required under a CAS-covered contract placed on or before December 31, 1995.

(5) Transition period waiver authority. For a CAS-covered contract to be awarded during the period January 1, 1996, through June 30, 1997, the awarding agency may waive the preaward Disclosure Statement submission requirement specified in 9903.202–1(f)(2) when a due date for the submission of a Disclosure Statement has previously been established by the cognizant Federal agency and the educational institution under the provisions of 9903.202–1(f) (3) and (4).

Caution: This waiver authority is not available unless the cognizant Federal agency and the educational institution have established a disclosure statement due date pursuant to a written agreement executed prior to January 1, 1996, and award is made prior to the established disclosure statement due date.

5352.225-9101 Logistics Support for Countries other than Germany

As prescribed in 5325.11111, insert a clause substantially the same as the following clause in solicitations and contracts:.

LOGISTICS SUPPORT FOR COUNTRIES OTHER THAN GERMANY (USAFE)(APR 2002)

(a) Logistics support as defined in the statement of work will be provided to authorized contractor employees and their dependents to the extent these services are available at the location where the contract is to be performed and as authorized by current applicable Air Force and European theater regulations, by current applicable international agreements and arrangements, by current policies, and the local installation commander. Lack of availability of any of these services shall not serve as a basis for claims by a contractor against the Government for increased cost of contract performance.

(b) An authorized contractor employee is defined as an employee who has been hired as a consequence of this contract and is employed at least 40 hours per week on this contract. For Italy, procedures must be

in accordance with the Memorandum of Understanding Between the Ministry of Defense of the Republic of Italy and The Department of Defense of the United States of America Concerning Use of Installations/Infrastructure by U.S. Forces in Italy, signed 2 February 1995. To qualify for Civilian Personnel status in Italy, the employee must (i) not be a stateless person; (ii) not be a national of any State which is not a Party to the North Atlantic Treaty; (iii) not be a national of Italy; (iv) not be ordinarily resident in Italy; and (v) be certified as a technical representative and issued a NATO SOFA Identification by the United States Sending State Office (USSSO) for Italy or by a base legal office with delegated authority. The final authority to determine whether an employee qualifies for Civilian Personnel status is USSSO.

(c) Any logistic support for other than NATO countries must comply with the International Agreement of the host nation.

(d) Abuse of Privileges. The Contractor will include a provision in his employment agreement with his employees to provide for disciplinary action, or discharge for cause, of the employee for any abuse of privileges authorized to herein. The US government retains the right to withdraw privileges as a result of Contractor employee abuse at no additional cost to the US government. This provision in no way will prohibit disciplinary action or legal prosecution by either the US government or the host country government. Services or privileges may be denied an individual basis at the discretion of the Installation Commander.

(e) The Contractor shall assure that upon termination or transfer of any employee who is granted logistic support, action is taken simultaneous with the termination of employment to assure that said employee ceases to have access to the services granted under logistic support. The Contractor shall assure that identification passes or other documents pertinent to or peculiar to the contract or privileges thereunder are turned over to the issuing office upon termination or transfer of any employee. The Contractor shall require a written receipt of such return and shall immediately forward a copy to the contracting officer.

(End of clause)

EXPORT CONTRACT ACT COMPLIANCE (DEC 2006)

The contractor shall assess the work to be performed in this effort to assure that all actions are in compliance with the Export Administration Regulations, 15 CFR Part 730 (EAR), of the Export Administration Act of 1979, 50 U.S.C. app. 2401-2420 (EAA). Technology listed in the Commerce Control List (CCL), 15 CFR Part 774, of the EAR shall not be exported or exposed to foreign nationals without the written consent of the U.S. Department of Commerce.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT

(a) The Government may extend the term of this contract by written notice to the Contractor within 60 days; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this

option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months.

(End of clause)

52.232-18 AVAILABILITY OF FUNDS (APR 1984)

Funds are not presently available for this contract. The Government's obligation under this contract is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are made available to the Contracting Officer for this contract and until the Contractor receives notice of such availability, to be confirmed in writing by the Contracting Officer.

(End of clause)

REPUBLIC OF KOREA (ROK) – STATUS OF FORCES AGREEMENT (SOFA) CONTRACT CLAUSE

INVITED CONTRACTOR OR TECHNICAL REPRESENTATIVE STATUS UNDER U.S. - REPUBLIC OF KOREA (ROK)

Invited Contractor (IC) and Technical Representative (TR) status shall be governed by the U.S. - ROK Status of Forces Agreement (SOFA) as implemented by United States Forces Korea (USFK) Reg 700-19, which can be found under the "publications" tab on the US Forces Korea homepage http://www.usfk.mil

(a) Definitions. As used in this clause—

"U.S. – ROK Status of Forces Agreement" (SOFA) means the Mutual Defense Treaty between the Republic of Korea and the U.S. of America, Regarding Facilities and Areas and the Status of U.S. Armed Forces in the Republic of Korea, as amended

"Combatant Commander" means the commander of a unified or specified combatant command established in accordance with 10 U.S.C. 161. In Korea, the Combatant Commander is the Commander, United States Pacific Command.

"United States Forces Korea" (USFK) means the subordinate unified command through which US forces would be sent to the Combined Forces Command fighting components.

"Commander, United States Forces Korea" (COMUSK) means the commander of all U.S. forces present in Korea. In the Republic of Korea, COMUSK also serves as Commander, Combined Forces Command (CDR CFC) and Commander, United Nations Command (CDR UNC).

"USFK, Assistant Chief of Staff, Acquisition Management" (USFK/FKAQ) means the principal staff office to USFK for all acquisition matters and administrator of the U.S.-ROK SOFA as applied to US and Third Country contractors under the Invited Contractor (IC) and Technical Representative (TR) Program (USFK Reg 700-19).

"Responsible Officer (RO)" means a senior DOD employee (such as a military E5 and above or civilian GS-7 and above), appointed by the USFK Sponsoring Agency (SA), who is directly responsible for determining and administering appropriate logistics support for IC/TRs during contract performance in the ROK.

(b) IC or TR status under the SOFA is subject to the written approval of USFK, Assistant Chief of Staff, Acquisition Management (FKAQ), Unit #15237, APO AP 96205-5237.

(c) The contracting officer will coordinate with HQ USFK/FKAQ, IAW FAR 25.8, and USFK Reg 700-19. FKAQ will determine the appropriate contractor status under the SOFA and notify the contracting officer of that determination.

(d) Subject to the above determination, the contractor, including its employees and lawful dependents, may be accorded such privileges and exemptions under conditions and limitations as specified in the SOFA and USFK Reg 700-19. These privileges and exemptions may be furnished during the performance period of the contract, subject to their availability and continued SOFA status. Logistics support privileges are provided on an as-available basis to properly authorized individuals. Some logistics support may be issued as Government Furnished Property or transferred on a reimbursable basis.

(e) The contractor warrants and shall ensure that collectively, and individually, its officials and employees performing under this contract will not perform any contract, service, or other business activity in the ROK, except under U.S. Government contracts and that performance is IAW the SOFA.

(f) The contractor's direct employment of any Korean-National labor for performance of this contract shall be governed by ROK labor law and USFK regulation(s) pertaining to the direct employment and personnel administration of Korean National personnel.

(g) The authorities of the ROK have the right to exercise jurisdiction over invited contractors and technical representatives, including contractor officials, employees and their dependents, for offenses committed in the ROK and punishable by the laws of the ROK. In recognition of the role of such persons in the defense of the ROK, they will be subject to the provisions of Article XXII, SOFA, related Agreed Minutes and Understandings. In those cases in which the authorities of the ROK decide not to exercise jurisdiction, they shall notify the U.S. military authorities as soon as possible. Upon such notification, the military authorities will have the right to exercise jurisdiction as is conferred by the laws of the U.S.

(h) Invited contractors and technical representatives agree to cooperate fully with the USFK Sponsoring Agency (SA) and Responsible Officer (RO) on all matters pertaining to logistics support and theater training requirements. Contractors will provide the assigned SA prompt and accurate reports of changes in employee status as required by USFK Reg 700-19.

(i) Theater Specific Training. Training Requirements for IC/TR personnel shall be conducted in accordance with USFK Reg 350-2 Theater Specific Required Training for all Arriving Personnel and Units Assigned to, Rotating to, or in Temporary Duty Status to USFK. IC/TR personnel shall comply with requirements of USFK Reg 350-2.

(j) Except for contractor air crews flying Air Mobility Command missions, all U.S. contractors performing work on USAF classified contracts will report to the nearest Security Forces Information Security Section for the geographical area where the contract is to be performed to receive information concerning local security requirements.

(k) Invited Contractor and Technical Representative status may be withdrawn by USFK/FKAQ upon:

(1) Completion or termination of the contract.

(2) Determination that the contractor or its employees are engaged in business activities in the ROK other than those pertaining to U.S. armed forces.

(3) Determination that the contractor or its employees are engaged in practices in contravention to Korean law or USFK regulations.

(l) It is agreed that the withdrawal of invited contractor or technical representative status, or the withdrawal of, or failure to provide any of the privileges associated therewith by the U.S. and USFK, shall not constitute grounds for excusable delay by the contractor in the performance of the contract and will not justify or excuse the contractor defaulting in the performance of this contract. Furthermore, it is agreed that withdrawal of SOFA status for reasons outlined in USFK Reg 700-19, Section II, paragraph 6 shall not serve as a basis for the contractor filing any claims against the U.S. or USFK. Under no circumstance shall the withdrawal of SOFA Status or privileges be considered or construed as a breach of contract by the U.S. Government.

(m) Support.

(1) Unless the terms and conditions of this contract place the responsibility with another party, the COMUSK will develop a security plan to provide protection, through military means, of Contractor personnel engaged in the theater of operations when sufficient or legitimate civilian authority does not exist.

(2)(i) All Contractor personnel engaged in the theater of operations are authorized resuscitative care, stabilization, hospitalization at level III military treatment facilities, and assistance with patient movement in emergencies where loss of life, limb, or eyesight could occur. Hospitalization will be limited to stabilization and short-term medical treatment with an emphasis on return to duty or placement in the patient movement system.

(ii) When the Government provides medical or emergency dental treatment or transportation of Contractor personnel to a selected civilian facility, the Contractor shall ensure that the Government is reimbursed for any costs associated with such treatment or transportation.

(iii) Medical or dental care beyond this standard is not authorized unless specified elsewhere in this contract.

(3) Unless specified elsewhere in this contract, the Contractor is responsible for all other support

required for its personnel engaged in the theater of operations under this contract.

(n) Compliance with laws and regulations. The Contractor shall comply with, and shall ensure that its personnel supporting U.S Armed Forces in the Republic of Korea as specified in paragraph (b)(1) of this clause are familiar with and comply with, all applicable—

(1) United States, host country, and third country national laws;

(2) Treaties and international agreements;

(3) United States regulations, directives, instructions, policies, and procedures; and

(4) Orders, directives, and instructions issued by the COMUSK relating to force protection, security, health, safety, or relationand interaction with local nationals. Included in this list are force protection advisories, health advisories, area (i.e. “off-limits”), prostitution and human trafficking and curfew restrictions.

(o) Vehicle or equipment licenses. IAW USFK Regulation 190-1, Contractor personnel shall possess the required licenses to operate all vehicles or equipment necessary to perform the contract in the theater of operations. All contractor employees/dependents must have either a Korean driver’s license or a valid international driver’s license to legally drive on Korean roads, and must have a USFK driver’s license to legally drive on USFK installations. Contractor employees/dependents will first obtain a Korean driver’s license or a valid international driver’s license then obtain a USFK driver’s license.

(p) Evacuation.

(1) If the COMUSK orders a non-mandatory or mandatory evacuation of some or all personnel, the Government will provide assistance, to the extent available, to United States and third country national contractor personnel.

(2) Non-combatant Evacuation Operations (NEO).
(i) The contractor shall designate a representative to provide contractor personnel and dependents information to the servicing NEO warden as required by direction of the Responsible Officer.

(ii) If contract period of performance in the Republic of Korea is greater than six months, non emergency essential contractor personnel and all IC/TR dependents shall participate in at least one USFK sponsored NEO exercise per year.

(q) Next of kin notification and personnel recovery.

(1) The Contractor shall be responsible for notification of the employee-designated next of kin in the event an employee dies, requires evacuation due to an injury, or is missing, captured, or abducted.

(2) In the case of missing, captured, or abducted contractor personnel, the Government will assist in personnel recovery actions in accordance with DOD Directive 2310.2, Personnel Recovery.

(3) IC/TR personnel shall accomplish Personnel Recovery/Survival, Evasion, Resistance and Escape

(PR/SERE) training in accordance with USFK Reg 525-40, Personnel Recovery

Procedures and USFK Reg 350-2 Theater Specific Required Training for all Arriving Personnel and Units Assigned to, Rotating to, or in Temporary Duty Status to USFK.

(r) Mortuary affairs. Mortuary affairs for contractor personnel who die while providing support in the theater of operations to U.S. Armed Forces will be handled in accordance with DOD Directive 1300.22, Mortuary Affairs Policy and Army Regulation 638-2, Care and Disposition of Remains and Disposition of Personal Effects.

(s) USFK Responsible Officer (RO). The USFK appointed RO will ensure all IC/TR personnel complete all applicable training as outlined in this clause.

(End of Clause)

7.0 APPLICABLE DOCUMENTS AND DEFINITIONS

7.1 Compliance Documents

The following documents provide specifications, standards, or guidelines that must be complied with in order to meet the requirements of this order, in each case the most recent version and date of document will apply:

- Institute of Electrical & Electronics Engineers (IEEE) 802 - Standards for Local and Metropolitan Area Networks: Overview and Architecture.
- Telecommunications Industry Association/Electronic Industries Alliance Standard TIA/EIA-606-A - Administration Standard for the Telecommunications Infrastructure of Commercial Buildings.
- J-STD-607-A - Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications (ANSI/J-STD--607-A - 2002)
- TIA/EIA - 568-B.1 – Commercial Building Telecommunications Cabling Standard – Part 1: General Requirements (ANSI/TIA/EIA-568-B.1-2001)
- TIA/EIA - 568-B.2 – Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components (ANSI/TIA/EIA-568-B.2-2001)
- TIA/EIA – 568-B.3 – Optical Fiber Cabling Components Standard (ANSI/TIA/EIA-568-B.3-2000)
- DoD Regulation 5200.2-R, “DoD Personnel Security Program,"
- DoD Regulation 5000.2-R, "Mandatory procedures for Major Defense Acquisition Programs (MDAP) and Major Automated Information System Acquisition Programs (MAISAPs)," Department of Defense Joint Technical Architecture,
- MHS Automated Information System (AIS) Security Policy Manual,
- MHS Architectural Framework,
- Building Industry Consulting Services International (BICSI), *Information Transport Systems Installation Manual (ITSIM),*
- Software Engineering Institute Capability Maturity Modeling (SEI CMM), Level 2 procedures and processes
- Army in Europe Regulation 715-9, “Contractor Personnel in Germany – Technical Expert, Troop Care & Analytical Support”

7.2 Reference Documents

The following documents may be helpful to the Contractor in performing the work described in this document:

- The documents listed above are also key reference documents

8.0 ATTACHMENTS Section Index:

A. Sites & Support Staff Requirement

B. MTF Network Infrastructure Description

C. Non-disclosure / Non-use Agreement

D. Organizational Conflict of Interest

E. Labor Category Responsibilities and Required Qualifications

F. Instructions for Contractor Access to DoD IT Systems

ATTACHMENT A – Sites & Support Staff Requirement

FTE	Location
CONUS – 68 FTEs	
Network Specialists	**AIR FORCE:** Altus AFB OK Barksdale AFB GA Cannon AFB NM Davis-Monthan AFB AZ Dover AFB DE Dyess AFB TX Edwards AFB CA Fairchild AFB WA Grand Forks AFB ND Hill AFB UT Holloman AFB NM Lackland AFB TX Little Rock AFB AR Los Angeles AFB CA Mountain Home AFB Nellis AFB NV Shaw AFB SC Sheppard AFB TX Tinker AFB OK Travis AFB CA Vandenberg AFB CA **ARMY:** Belvoir VA Benning GA Bliss TX Bragg NC Campbell KY Carson CO Drum NY Eustis VA Gordon (1) GA Hood TX Huachuca AZ Jackson SC Irwin CA Knox KY Leavenworth KS Leonard Wood MO Lewis WA Meade MD Polk LA Redstone AL Riley KS (2) Rucker GA Sam Houston TX

	Sill OK Stewart GA West Point NY **NAVY:** Bethesda MD Bremerton WA Great Lakes IL Groton RI Jacksonville FL Lejeune (2) NC Lemoore Naval Air Station CA Oak Harbor, WA Pendleton CA Pensacola FL Portsmouth VA San Diego CA **EI DNOC:** San Antonio TX (4) **GAL:** Auburn WA – Systems & Network Specialist Conus
Network Engineer	**EI:** San Antonio TX **GAL:** Auburn WA
OCONUS – Pacific – 12 FTEs	
Network Specialists	**AIR FORCE:** Kadena JP **ARMY:** Korea (3) – 1 MHS billet 1 Site-funded billet 1 Site-funded billet – Systems and Network Specialist Tripler Honolulu, HI Ft Wainwright AK Joint Base - Elmendorf-Richardson AK **NAVY:** Guam Okinawa JP Pearl Harbor, HI Yokosuka JP
Network Engineer	**EI Pacific Regional Office:** Korea
OCONUS – Europe – 7 FTEs	

Network Specialists	**ARMY:** Landstuhl GE Bavaria GE (base location is Vilseck) **NAVY:** Naples IT Rota SP Sigonella IT **TRICARE:** Sembach GE
Network Engineer	**EI Europe Regional Office**: Landstuhl, GE

ATTACHMENT B – MTF Network Infrastructure Description

A typical MTF network environment includes an array of protocols, operating systems and mediums such as:

- Transmission Control Protocol/Internet Protocol (TCP/IP)
- X-Window Display Manager (XDM)
- Hyper-Text Transfer Protocol (HTTP)
- Secure Hyper-Text Transfer Protocol (SHTTP)
- Simple Mail Transfer Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
- Domain Name Service (DNS)
- Dynamic Host Configuration Protocol (DHCP)
- Ethernet, Fast Ethernet, Gigabit Ethernet
- Asynchronous Transfer Mode (ATM)
- Fiber Distributed Data Interface (FDDI)
- Open Shortest Path First (OSPF)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Border Gateway Protocol (BGP)
- Windows Operating System versions NT/2000/2003/2008/XP/Win7/Win8 servers and workstations
- Open Virtual Memory System (OpenVMS) and UNIX in routed, switched and shared local area networks (LANs) that employ Cisco, Nortel, Enterasys, Alcatel and Foundry/Brocade equipment as well as various local and long-haul Integrated Services Digital Network (ISDN)
- 56 Kilobits per second (Kbps) through T1-T3 links, microwave, satellite and ATM wide area network (WAN) connectivity that employs channel service unit/data service unit (CSU/DSUs)
- Security suites employed at MTFs include Cisco firewalls and Cisco, Alcatel and NetScreen devices and Intrusion Detection Suites (IDSs)
- Cisco and/or Aruba wireless technology.

ATTACHMENT C: NON-DISCLOSURE / NON-USE AGREEMENT

Non-Disclosure Agreement for Contractor Employees and Subcontractors

I, _____, am an employee of or a subcontractor to _[Company Name]_, a contractor acting under contract to the __[Name of Directorate]__ under Prime Contract No. ____ , through Task Order _____. I understand that in the performance of this task, I may have access to sensitive or proprietary business, technical, financial, and/or source selection information belonging to the Government or other contractors. This information includes, but is not limited to, cost/ pricing data; Government spend plan data; Planning, Programming, Budgeting and Execution (PPBE) documents and information, as defined in DoD Directive 7045.14; contractor technical proposal data; independent government cost estimates; negotiation strategies and contractor data presented in negotiations; contracting plans and statements of work. I agree not to use, discuss, divulge, or disclose any such information or data to any person or entity except those persons directly concerned with the use or performance of this task order. I have been advised that the unauthorized disclosure, use or negligent handling of the information by me could cause irreparable injury to the owner of the information. The injury could be source sensitive procurement information of the government or proprietary/trade secret information of another company.

I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this agreement. Court costs and reasonable attorney fees incurred by the United States Government may be assessed against me if I lose such action. I understand that another company might file a separate claim against me if I have misused its proprietary information.

In the event that I seek other employment, I will reveal to any prospective employer the continuing obligation in this agreement *prior* to accepting any employment offer.

The obligations imposed herein do not extend to information/data which is:

a. in the public domain at the time of receipt or it came into the public domain thereafter through no act of mine;

b. disclosed with the prior written approval of the designated Contracting Officer;

c. demonstrated to have been developed by _[Company Name]_, or me independently of disclosures made hereunder;

d. disclosed pursuant to court order, after notification to the TMA designated Contracting Officer;

e. disclosed inadvertently despite the exercise of the same reasonable degree of care a party normally uses to protect its own proprietary information.

I have read this agreement carefully and my questions, if any, have been answered to my satisfaction.

ATTACHMENT D: ORGANIZATIONAL CONFLICT OF INTEREST

TRICARE Management Activity (TMA) has categorized all its non-purchased care requirements into three broad categories, as defined below, for purposes of identifying, avoiding or mitigating against Organizational Conflicts of Interest (OCIs) in accordance with FAR Subpart 9.5. These categories are defined as follows:

- Category 1: TMA Internal Support: Services which, by their very nature, give the Contractor access to extensive data about the contracts of all other TMA Contractors.

- Category 2: Program Management Support: Services which assist TMA in planning and managing its activities and programs. This includes, for example: requirements analysis, acquisition support, budget planning and management, business process reengineering, program planning and execution support, and independent technical management support.

- Category 3: Product Support. Services or end items required to meet the mission requirements of TMA's non-purchased care activities and programs. This includes, for example: concept exploration and development; system design; system development and integration; COTS procurement and integration; internal development testing; deployment; installation; operations; and maintenance.

Contractor participation in more than one of these areas may give rise to an unfair competitive advantage resulting from access to advance acquisition planning, source selection sensitive or proprietary information. Furthermore, Contractor participation in more than one area may give rise to a real or apparent loss of Contractor impartiality and objectivity where its advisory or planning assistance in one area potentially affects its present or future participation in another area.

The purpose of this categorization is to accomplish the following three objectives: (1) to inform prospective Offerors (Quoters) that TMA presumes that award of a contract or order in the subject category will give rise to real or apparent OCIs with respect to requirements in the other two categories; (2) to assist current Contractors and prospective Offerors in developing their own business strategies regarding participation in TMA requirements and in identifying and, where possible, avoiding or mitigating against OCIs; and (3) to ensure that all current Contractors and prospective Offerors are afforded the maximum practicable opportunity to compete for all TMA requirements consistent with the restrictions required under FAR Subpart 9.5 and sound business practices.

For purposes of identifying, avoiding and / or mitigating against OCIs, TMA will examine all its non-purchased care requirements and acquisitions regardless of the cognizant contracting activity (e.g., USAMRAA, GSA, other agency Multiple Award Schedules, etc.) or the type of contract vehicle used (e.g., FSS order, Fair Opportunity competitive order under Multiple Award ID/IQ Contracts, competitively negotiated awards under FAR Part 15, etc.).

Each TMA non-purchased care solicitation will therefore be designated as falling within one of the three above defined categories. The work called for under this contract / order has been determined by TMA to fall within the following non-purchased care OCI category:

Category 3: Product Support

TMA will administer this clause for purposes of award eligibility for each solicitation as follows:

An Offeror that has never provided support to TMA in any of the categories is eligible for award in any category without any further action required under this clause.

An Offeror that provides or has provided support to TMA in only one category of work and has never supported TMA in any other category (a single-category Contractor) is eligible for award for any future requirement in that single category without further action under this clause.

A single-category Offeror/Contractor wishing to submit an offer in a different category, or any Offeror/Contractor which now provides or previously has provided support in more than one category, *must include the following as part of its offer*:

- Perform a comparative analysis of the potential new work against *all* current and previous work performed in support of TMA in *any category other than that of the new work being offered*. The comparative analysis must be included in the quote for the new work, and must include a statement certifying whether the Contractor believes that its performance of the quoted new work would create a real or apparent OCI. If the Contractor believes that no real or perceived OCI will result from an award of the quoted work, no additional action by the Contractor is required.

- If the Offeror/Contractor believes that a real or apparent OCI may exist as a result of an award, the Contractor shall also submit an OCI Avoidance or Mitigation Plan with its quote.

Inclusion of the comparative analysis and OCI Avoidance or Mitigation Plan will not be counted against any offer page limitations otherwise stated in the solicitation.

The Contracting Officer (and when applicable the appropriate program office, acquisition manager, and legal counsel) will review the comparative analysis and, if provided, the Avoidance or Mitigation Plan, in accordance with the requirements of FAR Subpart 9.5 (Organizational Conflict of Interest) to determine whether award to that Offeror would be consistent with those requirements. If it is unilaterally determined by the Contracting Officer that no OCI would arise or that the OCI Avoidance or Mitigation Plan adequately protects the interests of the government in the event of award to that Offeror, the Offeror will be determined, for purposes of this clause, to be eligible for award. If the Contracting Officer reasonably determines that a Contractor has not provided either a comparative analysis or avoidance/mitigation plan, or both, or that the analyses or plan provided is inadequate, sanctions including elimination from the award process, or termination of the related contract effort already awarded, as well as other appropriate actions will be considered.

If the Offeror/Contractor knows of no OCI in accepting work under this contract, it shall certify its OCI status and submit the certification at the end of this clause with its quote and any later award, if awarded the contract. The Contractor shall also obtain a similar certification of OCI status from all subcontractors, teaming partners or consultants prior to tasking any such party under this contract. The Contractor shall appropriately modify and include this clause, including this paragraph, in all consulting agreements and subcontracts of any tier to preserve the rights of the Government.

For breach of any of the above restrictions or for nondisclosure or misrepresentation of any relevant facts required to be disclosed concerning this contract, the Government may terminate this contract, disqualify the Contractor from subsequent related contractual efforts, and pursue any remedies as may be permitted by law or this contract.

Prior to a contract modification involving a change to the Statement of Work, or an increase in the level of effort or extension of the term of the contract, the Contractor shall submit any applicable organizational conflict of interest disclosure or an update of the previously submitted disclosure or representation.

The Offeror/Contractor should review the considerations below in determining whether or not a conflict of interest exists.

- Does the Offeror or any intended subcontractors, teaming partners, quoted employees, or affiliates have Unequal Access to Information? Would award to the Offeror result in the Offeror having the opportunity to access nonpublic information that may give the Offeror a competitive

advantage in a later competition for a government contract? Specifically, will the Offeror/Contractor have access to any of the following information:

- Budget(s), or Budget Information?
- Acquisition Sensitive Information related to the procurement process to include, but not limited to Acquisition Plans, Requirements, Statements of Work, or Evaluation Criteria?

- Does the Offeror or any intended subcontractors, teaming partners, quoted employees, or affiliates have "*impaired objectivity*" because the Offeror's ability to render impartial judgments may be compromised because of its conflicting role(s) on this effort and other government contracts?

- Do "*biased ground rules*" exist? Most commonly, this would include a situation where the Offeror has, as a government Contractor, written specifications or a statement of work for this effort, which could skew competition in favor of itself?

- Is the Offeror aware of any other information relating to this quoted contract/order, which could reasonably be construed as creating an OCI?

The Offeror/Contractor hereby certifies to the best of its knowledge its OCI status below:

(Offeror: Choose <u>one</u> of the following two statements. Indicate which one applies by placing an X in the box to the left of the statement.)

☐ No real or perceived OCI, as defined in FAR 2.1 and discussed in FAR 9.5, will result from an award of the quoted work (there are no 'Yes' responses to the questions above).

☐ A real or apparent OCI may exist as a result of an award and therefore an appropriate OCI Avoidance or Mitigation Plan is attached (Offeror shall include an appropriate OCI Avoidance or Mitigation Plan, as required by this clause, with its quote to the Contracting Officer).

Upon award the Contractor agrees that it will provide timely OCI training to all employees and subcontractor employees working on this effort, which will include emphasis on how work performed by Contractor employees (either prime Contractor, subcontractor, or other teaming partners) under one TMA OCI category can exclude the Contractor as well as its teaming partners from performing related tasks under a different OCI category of work.

_____ (Signature) _____ (Date)

_____ (Printed Name) _____ (Title)

ATTACHMENT E: LABOR CATEGORY RESPONSIBILITIES AND REQUIRED QUALIFICATIONS

JOB TITLE: *Senior Network Engineer for CONUS*

RESPONSIBILITIES:

The Senior Network Engineer for CONUS region supports the medical mission of the DoD and ensures that the highly complex and technical requirements related to the infrastructure are addressed. The Senior Network Engineer is a key personnel, and identifies and resolves larger, more complex LAN/WAN network problems and issues, researches network-level problems using network management tools and is responsible for providing high-level installation, configuration, management and troubleshooting of LAN/WAN communication equipment for networked facilities. Serves as the premier Network Specialist for this contract; subject matter expert for all issues covered under the other jobs discussed within.

Serves as the CONUS, as well as global, point of contact for network issues, configuration management and communications interconnection, addressing, and multi-protocol routing and network management.

Advises and consults with government staff, agencies and Contractor representatives involved with LAN/WAN design, network implementation and network management to ensure the LAN/WAN adequately supports the MHS mission and provides optimal performance. Interfaces with and leads Network Specialists and internal or external organizations to resolve LAN/WAN issues.

The Senior Network Engineer for CONUS region is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Hewlett Packard (HP) OpenView, Cisco Works and Tivoli. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WAN security in maintaining the LAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Senior Network Engineer must be capable of establishing and configuring network firewalls, VPN devices and IDSs.

Provides recommendations to personnel in the field by making either a change to network level operations or an enhancement to the network (tuning or upgrade). Studies vendor products to determine which components and configurations best meet the requirements of DoD and MTFs. Establishes and implements LAN/WAN procedures and standards to ensure compliance with DoD and Command objectives and policies. Communicates with key customers on the status of all network support requests.

Beyond network design and implementation, the engineer continuously evaluates and resolves complex technical issues associated with network and routing protocols at all levels of the Open Systems Interconnection (OSI) model through the use of diagnostics and network administration tools. Provides proactive input on policies and issues related to standardization as well as develop and write policies and procedures that identify best practice solutions necessary for operations in support of the LAN/WAN. Defines and establishes minimum standards related to LAN/WAN access and its impact on overall network operations. Leads/participates on other projects and support as the need arises.

QUALIFICATIONS:

Compliance with Department of Defense (DoD) Directive 8570.01 “Information Assurance Training, Certification, and Workforce Management” is required. Information Assurance Manager (IAM) Level III or equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" (most recent version) is required.

Ability to carry out functions of all subordinate positions listed in this Labor Category synopsis, should the individual be tasked with traveling to any site covered by this contract.

EXPERIENCE: The Senior Network Engineer for the CONUS region must have a clear understanding of TCP/IP, XDM, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate knowledge of synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications is also required.

Possess experience in routed, switched and shared LAN environments that operate such items as Microsoft Windows NT/2000/2003/XP/Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul ISDN, T1, T3, satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*one of the following three (3) options is required*):

- Bachelor’s degree in computer sciences, engineering, or related technical discipline, and five (5) years of directly related experience
- Successful completion of a certification program at a technical or vocational school, and ten (10) .years of directly related, progressively complex experience
- Comparable Department of Defense technical training , and ten (10) years of directly related, progressively complex experience

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience with DoD Health Care Information Systems is required. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems, and HP Openview. Microsoft Certified Systems Engineer (MCSE) is desire; Cisco Certified Network Professional (CCNP) and Certified Information Systems Security Professional (CISSP) is required.

BACKGROUND: An Automated Data Processing (ADP) sensitivity Level I determination and a **“SECRET”** security level designation is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must be able to communicate effectively with a broad audience to include Government officials, medical professionals and highly specialized technical personnel, both verbally and in writing.

JOB TITLE: ***Senior Network Engineer for Pacific Region***

RESPONSIBILITIES:

The Senior Network Engineer for the Pacific region supports the medical mission of the DoD and ensures that the highly complex and technical requirements related to the infrastructure are addressed. The Senior Network Engineer is a key personnel, and identifies and resolves larger, more complex LAN/WAN network problems and issues, researches network-level problems using network management tools and is responsible for providing high-level installation, configuration, management and troubleshooting of LAN/WAN communication equipment for networked facilities.

Serves as the regional point of contact for network issues, configuration management and communications interconnection, addressing, and multi-protocol routing and network management.

Advises and consults with government staff, agencies and Contractor representatives involved with LAN/WAN design, network implementation and network management to ensure the LAN/WAN adequately supports the MHS mission and provides optimal performance. Interfaces with and leads Network Specialists and internal or external organizations to resolve LAN/WAN issues.

The Senior Network Engineer for the Pacific region is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Hewlett Packard (HP) OpenView, Cisco Works and Tivoli. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WAN security in maintaining the LAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Senior Network Engineer must be capable of establishing and configuring network firewalls, VPN devices and IDSs.

Provides recommendations to personnel in the field by making either a change to network level operations or an enhancement to the network (tuning or upgrade). Studies vendor products to determine which components and configurations best meet the requirements of DoD and MTFs in the Pacific region. Establishes and implements LAN/WAN procedures and standards to ensure compliance with DoD and Pacific Regional Command objectives and policies. Communicates with key customers on the status of all network support requests.

Beyond network design and implementation, the engineer continuously evaluates and resolves complex technical issues associated with network and routing protocols at all levels of the Open Systems Interconnection (OSI) model through the use of diagnostics and network administration tools. Provides proactive input on policies and issues related to standardization as well as develop and write policies and procedures that identify best practice solutions necessary for operations in support of the LAN/WAN. Defines and establishes minimum standards related to LAN/WAN access and its impact on overall network operations. Leads/participates on other projects and support as the need arises.

QUALIFICATIONS:

Compliance with Department of Defense (DoD) Directive 8570.01 “Information Assurance Training, Certification, and Workforce Management” is required. Information Assurance Manager (IAM) Level III or

equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" (most recent version) is required.

EXPERIENCE: The Senior Network Engineer for the Pacific region must have a clear understanding of TCP/IP, XDM, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate knowledge of synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications is also required.

Possess experience in routed, switched and shared LAN environments that operate such items as Microsoft Windows NT/2000/2003/XP/Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul ISDN, T1, T3, satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*One of the following three (3) options is required*):

- Bachelor's degree in computer sciences, engineering, or related technical discipline, and five (5) years of directly related experience
- Successful completion of a certification program at a technical or vocational school, and ten (10) .years of directly related, progressively complex experience
- Comparable Department of Defense technical training , and ten (10) years of directly related, progressively complex experience

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience with DoD Health Care Information Systems is required. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems, and HP Openview. Microsoft Certified Systems Engineer (MCSE) is desired; Cisco Certified Network Professional (CCNP) and Certified Information Systems Security Professional (CISSP) is required.

BACKGROUND: An Automated Data Processing (ADP) sensitivity Level I determination and a **"SECRET"** security level designation is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must be able to communicate effectively with a broad audience to include Government officials, medical professionals and highly specialized technical personnel.

JOB TITLE: ***Senior Network Engineer for EUROPE***

RESPONSIBILITIES:

The Senior Network Engineer for Europe supports the medical mission of the DoD and ensures that the highly complex and technical requirements related to the infrastructure are addressed. The (Senior) Network Engineer is a key personnel, and identifies and resolves larger, more complex LAN/WAN network problems and issues, researches network-level problems using network management tools and is responsible for providing high-level installation, configuration, management and troubleshooting of LAN/WAN communication equipment for networked facilities.

Serves as the regional point of contact for network issues, configuration management and communications interconnection, addressing, and multi-protocol routing and network management.

Advises and consults with government staff, agencies and Contractor representatives involved with LAN/WAN design, network implementation and network management to ensure the LAN/WAN adequately supports the MHS mission and provides optimal performance. Interfaces with and leads Network Specialists and internal or external organizations to resolve LAN/WAN issues.

The Senior Network Engineer for Europe is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Hewlett Packard (HP) OpenView, Cisco Works and Tivoli. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WAN security in maintaining the LAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the (Senior) Network Engineer must be capable of establishing and configuring network firewalls, VPN devices (NetScreen knowledge desirable), and IDSs.

Provides recommendations to personnel in the field by making either a change to network level operations or an enhancement to the network (tuning or upgrade). Studies vendor products to determine which components and configurations best meet the requirements of DoD and European MTFs. Establishes and implements LAN/WAN procedures and standards to ensure compliance with DoD and European Regional Command objectives and policies. Communicates with key customers on the status of all network support requests.

Beyond network design and implementation, the engineer continuously evaluates and resolves complex technical issues associated with network and routing protocols at all levels of the Open Systems Interconnection (OSI) model through the use of diagnostics and network administration tools. Provides proactive input on policies and issues related to standardization as well as develop and write policies and procedures that identify best practice solutions necessary for operations in support of the LAN/WAN. Defines and establishes minimum standards related to LAN/WAN access and its impact on overall network operations. Leads/participates on other projects and support as the need arises.

QUALIFICATIONS:

Compliance with Department of Defense (DoD) Directive 8570.01 “Information Assurance Training, Certification, and Workforce Management” is required. Information Assurance Manager (IAM) Level III or equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" (most recent version) is required.

EXPERIENCE: The Senior Network Engineer for Europe must have a clear understanding of TCP/IP, IPX/SPX, XDM, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate knowledge of synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications is also required.

Possess experience in routed, switched and shared LAN environments that operate such items as Novell Netware, Microsoft Windows NT/2K/XP, UNIX, LINUX, and OpenVMS and employ routers, switches, hubs and terminal servers as well as various local and long-haul ISDN, T1, T3, (European E1 – E3 desirable) satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*One of the following three (3) options is required*):

- Bachelor's degree in computer sciences, engineering, or related technical discipline, and five (5) years of directly related experience
- Successful completion of a certification program at a technical or vocational school, and ten (10) .years of directly related, progressively complex experience
- Comparable Department of Defense technical training , and ten (10) years of directly related, progressively complex experience

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience with DoD Health Care Information Systems is required. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems and HP Openview. Capability and/or understanding of software scripting (e.g. Perl). Microsoft Certified Systems Engineer (MCSE) is desire; Cisco Certified Network Professional (CCNP) and Certified Information Systems Security Professional (CISSP) is required.

BACKGROUND: An Automated Data Processing (ADP) sensitivity Level I determination is required for this position. A **"SECRET"** security level designation is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must be able to communicate effectively with a broad audience to include Government officials, medical professionals and highly specialized technical personnel.

JOB TITLE: ***Network Specialist***

RESPONSIBILITIES:

The Network Specialist ensures that the LAN/WAN is capable of providing required services by supporting the network infrastructure through the use of troubleshooting and problem resolution in a production environment. Provides daily operational support for LAN/WAN networks, including firewalls. Plans, installs and supports hardware and software upgrades.

The Network Specialist is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Hewlett Packard (HP) OpenView, Cisco Works and Tivoli. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for maintaining LAN – WAN barrier systems to prevent unauthorized access to MTF systems. In order to meet these requirements, the Network Specialist must be familiar with Cisco firewalls, Cisco, Alcatel, Hewlett-Packard, Nortel and NetScreen VPN devices and IDSs.

Uses diagnostic utilities to identify and isolate problems encountered on different mediums and network protocols, gather latency statistics and find specific network bottlenecks, evaluate problems and implement fix actions through device reconfiguration or replacement depending on the circumstances.

QUALIFICATIONS:

Compliance with Department of Defense (DoD) Directive 8570.01 “Information Assurance Training, Certification, and Workforce Management” is required. Information Assurance Technical (IAT) Level II or equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" (most recent version) is required.

EXPERIENCE: The Network Specialist must have a clear understanding of TCP/IP, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, EIGRP, OSPF, PPP, HDLC, V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications, EIA/TIA cable standards and Internet standards. The Network Specialist must address issues related to synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Required experience with various OTDR, cable testers, network sniffers.

Possess experience in routed, switched and shared LAN environments that operate Novell Netware, Microsoft Windows NT/2000/2003/XP/Active Directory, UNIX and OpenVMS and employ various routers switches, hubs and terminal servers as well as various local and long-haul ISDN,256 Kbps through T1 - T3, satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*One of the following three (3) options is required*):

- Bachelor’s degree in a technical discipline such as computer sciences, and three (3) years related experience
- Successful completion of a certification program at a technical or vocational school, and eight (8) years related experience.

- Comparable Department of Defense technical training , and eight (8) years of directly related, progressively complex experience

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems and HP Openview desired. Has the following certifications aligned to site network architecture: Security+ and Cisco Certified Network Associate (CCNA) or equivalent (ie, BCNE for Brocade, etc).

BACKGROUND: An Automated Data Processing (ADP) sensitivity level II determination is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

JOB TITLE: ***LAN (Network) Specialist (Landstuhl, Germany & Bavaria, Germany)***

RESPONSIBILITIES:

The LAN Specialist ensures that the LAN/WAN is capable of providing required services by supporting the network infrastructure through the use of troubleshooting and problem resolution in a production environment. Provides daily operational support for LAN/WAN networks, including firewalls. Plans, installs and supports hardware and software upgrades.

The LAN Specialist is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Hewlett Packard (HP) OpenView, Cisco Works and Tivoli. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for maintaining LAN – WAN barrier systems to prevent unauthorized access to MTF systems. In order to meet these requirements, the Network Specialist must be familiar with Cisco firewalls, Cisco, Alcatel and Avaya VPN devices and IDSs.

Uses diagnostic utilities to identify and isolate problems encountered on different mediums and network protocols, gather latency statistics and find specific network bottlenecks, evaluate problems and implement fix actions through device reconfiguration or replacement depending on the circumstances.

QUALIFICATIONS:

Compliance with Department of Defense (DoD) Directive 8570.01 “Information Assurance Training, Certification, and Workforce Management” is required. Information Assurance Technical (IAT) Level II or equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" (most recent version) is required.

EXPERIENCE: The LAN Specialist must have a clear understanding of TCP/IP, IPX/SPX, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, EIGRP, OSPF, PPP, HDLC, V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications, EIA/TIA cable standards and Internet standards. The LAN Specialist must address issues related to synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Required experience with various OTDR, cable testers, network sniffers.

Possess experience in routed, switched and shared LAN environments that operate Novell Netware, Microsoft Windows NT/2000, UNIX and OpenVMS and employ various routers switches, hubs and terminal servers as well as various local and long-haul ISDN,56 Kbps through T1 - T3 **(European E1 – E3 experience desired)**, satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*One of the following three (3) options is required*):

- Bachelor’s degree in computer sciences, engineering, or related technical discipline, and five (5) years related experience
- Successful completion of a certification program at a technical or vocational school, and ten (10) years related experience.

- Comparable Department of Defense technical training, and ten (10) years of related experience.

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems and HP Openview desired. Has the following certifications aligned to site network architecture: Security+ and Cisco Certified Network Associate (CCNA) or equivalent.

BACKGROUND: An Automated Data Processing (ADP) sensitivity level II determination is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

JOB TITLE: ***Systems and Network Specialist (CONUS)***

RESPONSIBILITIES:

Provides computer systems maintenance and repair. Maintains servers, software systems and networks. Diagnoses and resolves hardware, software, firmware and network problems. Configures, maintains and upgrades network connection devices, network hardware/software equipment, and automation equipment.

The system and network administrator performs system design for site systems and system components. Maintains, operates, and evaluates desktop, network and communications hardware and software plus the system requirements needed to keep the Local Area Network operational at the indicated percentages. Analyzes ongoing operation of Local Area Network and Wide Area Network system(s) to ensure the hardware and network operating software are functioning properly and operating standards are met. Troubleshoots the Local Area Network, the Wide Area Network, and other network related problems. Coordinates and collaborates with support staff of the host network and all other applicable agencies. Manages, maintains, and supports the development of a standard workstation configuration to be used across all site systems in accordance with Department of Defense and host network regulations. Provides Helpdesk support to on-site users, using available resources to successfully diagnose and resolve problems with desktop computers, laptops, peripherals, commonly used office applications and other information technology as needed. Supports other telecommunication systems as needed, such as telephones, video teleconference systems, etc.

QUALIFICATIONS:

EXPERIENCE: Must have a clear understanding of TCP/IP, IPX/SPX, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, EIGRP, OSPF, PPP, HDLC, V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications, EIA/TIA cable standards and Internet standards. Must address issues related to synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Required experience with various cable testers and network sniffers.

Possesses understanding of routed, switched and shared LAN environments that operate Microsoft Windows NT/2000, VMWare, UNIX and OpenVMS and employ various routers switches, hubs and terminal servers as well as various local and long-haul ISDN,56 Kbps through T1 - T3, satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*One of the following three (3) options is required*):

- Bachelor’s degree in a technical discipline such as computer sciences, and three (3) years related experience
- Successful completion of a certification program at a technical or vocational school, and eight (8) years related experience.
- Comparable Department of Defense technical training , and eight (8) years of directly related, progressively complex experience

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. MCSE, BCNE, and/or CCNA preferred but not required. Expertise in Windows networks, Cisco Systems, and HP Openview desired. Has or can obtain the following certifications: Department of Defense (DoD) Information Assurance Technical Level 2 or equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" most recent version, within 180 days after contract award or arrival in Theater (whichever is later).

BACKGROUND: An Automated Data Processing (ADP) sensitivity level II determination is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

JOB TITLE: ***Systems and Network Specialist (Sembach, Germany)***

RESPONSIBILITIES:

Provides computer systems maintenance and repair. Maintains servers, software systems and networks. Diagnoses and resolves hardware, software, firmware and network problems. Configures, maintains and upgrades network connection devices, network hardware/software equipment, and automation equipment.

The system and network administrator performs system design for TRICARE Area Office - Europe systems and system components. Maintains, operates, and evaluates desktop, network and communications hardware and software plus the system requirements needed to keep the Local Area Network operational at the indicated percentages. Analyzes ongoing operation of Local Area Network and Wide Area Network system(s) to ensure the hardware and network operating software are functioning properly and operating standards are met. Troubleshoots the Local Area Network, the Wide Area Network, and other network related problems. Coordinates and collaborates with support staff of the host network and all other applicable agencies. Manages, maintains, and supports the development of a standard workstation configuration to be used across all TRICARE Area Office - Europe systems in accordance with Department of Defense and host network regulations. Provides Helpdesk support to on-site users, using available resources to successfully diagnose and resolve problems with desktop computers, laptops, peripherals, commonly used office applications and other information technology as needed. Supports other telecommunication systems as needed, such as telephones, video teleconference systems, etc.

QUALIFICATIONS:

EXPERIENCE: Must have a clear understanding of TCP/IP, IPX/SPX, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, EIGRP, OSPF, PPP, HDLC, V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications, EIA/TIA cable standards and Internet standards. Must address issues related to synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Required experience with various cable testers and network sniffers.

Possesses understanding of routed, switched and shared LAN environments that operate Microsoft Windows NT/2000, UNIX and OpenVMS and employ various routers switches, hubs and terminal servers as well as various local and long-haul ISDN,56 Kbps through T1 - T3 **(European E1 – E3 experience desired)**, satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*One of the following three (3) options is required*):

- Bachelor's degree in computer sciences, engineering, or related technical discipline, and five (5) years related experience.
- Successful completion of a certification program at a technical or vocational school, and five (5) years related experience.
- Comparable Department of Defense technical training, and five (5) years related experience.

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. MCSE, BCNE, and/or CCNA preferred but not required. Expertise in Windows networks, Cisco Systems, and HP Openview desired. Has or can obtain the following certifications: Department of Defense (DoD) Information Assurance Technical Level 2 or equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" most recent version, within 180 days after contract award or arrival in Theater (whichever is later)
.

BACKGROUND: An Automated Data Processing (ADP) sensitivity level II determination is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

JOB TITLE: *Systems and Network Specialist (Yongsan (Seoul) Korea)*
RESPONSIBILITIES:

Provides computer systems maintenance and repair. Maintains servers, software systems and networks. Diagnoses and resolves hardware, software, firmware and network problems. Configures, maintains and upgrades network connection devices, network hardware/software equipment, and automation equipment.

The system and network administrator performs system design for Brian Allgood Army Community Hospital systems and system components. Maintains, operates, and evaluates desktop, network and communications hardware and software plus the system requirements needed to keep the Local Area Network operational at the indicated percentages. Analyzes ongoing operation of Local Area Network and Wide Area Network system(s) to ensure the hardware and network operating software are functioning properly and operating standards are met. Troubleshoots the 'Local Area Network', the 'Wide Area Network', and other network related problems. Coordinates and collaborates with support staff of the host network and all other applicable agencies. Manages, maintains, and supports the development of a standard workstation configuration to be used across all affected administrative ADP systems in accordance with Department of Defense and host network regulations. Provides Helpdesk support to onsite users, using available resources to successfully diagnose and resolve problems with desktop computers, laptops, peripherals, commonly used office applications and other information technology as needed. Supports other telecommunication systems as needed, such as telephones, video teleconference systems, etc.

QUALIFICATIONS:

EXPERIENCE: Must have a clear understanding of TCP/IP, IPX/SPX, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, EIGRP, OSPF, PPP, HDLC, V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications, EIA/TIA cable standards and Internet standards. Must address issues related to synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Required experience with various cable testers and network sniffers.

Possesses understanding of routed, switched and shared LAN environments that operate Microsoft Windows NT/2000, UNIX and OpenVMS and employ various routers switches, hubs and terminal servers as well as various local and long-haul ISDN, 56 Kbps through T1 - T3 **(Asian E1 – E3 experience desired)**, satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION (*One of the following three (3) options is required*):

- Bachelor's degree in computer sciences, engineering, or related technical discipline, and five (5) years related experience.
- Successful completion of a certification program at a technical or vocational school, and five (5) years related experience.
- Comparable Department of Defense technical training, and five (5) years related experience.

Any degree or non-Department of Defense certification must be from a college, university, technical or vocational school that has obtained accreditation by a regionally or nationally recognized accrediting

agency (e.g. North Central Association of Colleges and Schools - The Higher Learning Commission; Southern Association of Colleges and Schools - Commission on Colleges; Middle States Commission on Higher Education, etc.).

OTHER SKILLS: Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. MCSE, BCNE, and/or CCNA preferred but not required. Expertise in Windows networks, Cisco Systems, and HP Openview desired. Has or can obtain the following certifications: Department of Defense (DoD) Information Assurance Technical Level 2 or equivalent certification, per DoD 8570.01-M, "Information Assurance Workforce Improvement Program" most recent version, within 180 days after contract award or arrival in Theater (whichever is later).

BACKGROUND: An Automated Data Processing (ADP) sensitivity level determination may be required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

ATTACHMENT F

TRICARE Management Activity

Office of Administration, Personnel Security Division

Instructions for Contractor Access to DoD IT Systems

I. BACKGROUND

The Department of Defense (DoD) requires contractor personnel designated for assignment to an ADP/IT position to undergo a successful security screening before being granted access to DoD information technology (IT) systems that contain sensitive data. Contractor personnel in positions requiring access to the following must be designated as ADP/IT-I or ADP/IT-II:

- Access to a secure DoD Facility
- Access to a DoD Information System (IS) or a DoD Common Access Card (CAC)-enabled network
- Access to DEERS or the B2B Gateway.

Effective October 1, 2009, DoD transitioned to the Electronic Questionnaires for Investigations Processing (e-QIP) for the processing of investigative Standard Forms (SFs) to include SF-85 (Questionnaire for Non-Sensitive Positions), SF-85P (Questionnaire for Public Trust Positions), and SF-86 (Questionnaire for National Security Positions). e-QIP is a web-based automated system managed by the Office of Personnel Management (OPM), which facilitates the processing of SFs for background investigations. Most companies having TRICARE contracts have positions of Public Trust and require the submission of the SF-85P. These companies will be phased-in to e-QIP by the TMA, Office of Administration, Personnel Security Division (TMA PSD). The TMA PSD shall provide each Facility Security Officer (FSO) the training necessary to access and use e-QIP.

As previously noted, contractor personnel are required to have a favorably completed background investigation in accordance with their position designations. However, the TMA PSD may approve an interim DoD CAC to contractor personnel for access to DoD IT systems. Approval for an interim DoD CAC is based on a favorable advance National Agency Check (NAC), Federal Bureau of Investigation (FBI) fingerprint check, and an initiated background investigation through e-QIP with OPM.

In order to safeguard against inappropriate use and disclosure of sensitive information, the following references and guidance are used by TMA as source documents:

- Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- DoD 6025.18-R, "DoD Health Information Privacy Regulation, January 2003
- DoD 5200.2-R, "DoD Personnel Security Program, January 1987
- DoD 5400.11-R, "Department of Defense Privacy Program, May 14, 2007)
- DoDI 8500.1, "Information Assurance (IA)", October 24, 2002
- Homeland Security Presidential Directive 12 (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
- Federal Information Processing Standards Publication 201 (FIPS 201-1), Personal Identify Verfication (PIV) of Federal Employees and Contractors, March 2006
- Directive Type Memorandum (DTM) 08-006, DoD Implementation of Homeland Security Presidential Directive -12 (HSPD-12), November 26, 2008
- Request for Waiver to Grant Interim Access to DoD Information Systems for TRICARE Contractor Employees, May 14, 2009

The requirements above must be met by contractors and subcontractors who have access to DoD IS containing information protected by the Privacy Act of 1974 and Protected Health Information (PHI) under HIPAA.

II. PURPOSE

The purpose of this instruction is to define the Contractor's responsibilities when contractor personnel require access to DoD IT systems.

III. SCOPE OF WORK

A. **Contract/Order.** Upon notification that a contract/order has been awarded, the Contractor awarded the contract/order shall:

(1) Contact the TMA PSD and provide its company name, mailing address, e-mail address, telephone number, fax number, and the name of its designated official or Facility Security Officer (FSO).

(2) Provide its contract number, delivery order number, and contract beginning and ending dates.

B. **ADP/IT Position Sensitivity Designations.** The Prime Contractor shall ensure all contractor personnel, including any subcontractor personnel, are designated as ADP/IT-I or ADP/IT-II when their duties meet the criteria of the position sensitivity designations. The Contractor FSO shall use the guidance below to determine a contractor employee's specific ADP/IT level.

(1) **ADP/IT-I –** Those positions which have major responsibility for the planning, direction, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software; or responsibility for the preparation or approval of data for input into a system with relatively high risk for effecting severe damage to persons, properties or systems, or realizing significant personal gain.

A Single Scope Background Investigation (SSBI) is the type of investigation used for ADP/IT-I Trustworthiness Determinations. The scope of the SSBI is 10 years and includes:

- Personal Subject Interview (conducted by an OPM Investigator)
- Standard National Agency Check (NAC)*
- Employment, education, residence, and reference checks
- Law enforcement and court record checks
- Check of citizenship and family's legal status (if foreign born)
- Check of spouse or cohabitants, and former spouse (if applicable)
- Credit check

(2) **ADP/IT-II –** Those positions which have the responsibility for systems' design, operation, testing, maintenance, and/or monitoring, but are carried out under the technical review of an ADP/IT-I. Responsibilities include but are not limited to access to and / or processing of proprietary data requiring protection under the Privacy Act of 1974 or Government-developed privileged information involving the award of contracts.

A National Agency Check with Local Law and Credit (NACLC) is the type of investigation used for ADP/IT-II Trustworthiness Determinations. The scope of the NACLC is 7 years and includes the following:

- Standard NAC*
- Employment, education, residence, and reference checks
- Law enforcement check
- Credit check

**Standard NAC includes: SII, DCII, FBI name check, and FBI National Crime History fingerprint check*

Within 5-business days of notification of a contract award, the Contractor FSO shall notify and provide the Contracting Officer Representative (COR) with a list of contractor employees who require access to DoD IT systems. For each contractor employee, the list shall include the individual's name, social security number, date of birth, and the ADP/IT level.

C. **Employee Prescreening.** The Contractor shall conduct thorough reviews of information submitted on an individual's application for employment in a position that requires an ADP/IT background investigation or involves access via a contractor system to data protected by either the Privacy Act of 1974, as amended, or the HHS HIPAA Privacy and Security Final Rule. This prescreening shall include reviews that:

- Verify United States citizenship
- Verify education (degrees and certifications) required for the position in question
- Screen for negative criminal history at all levels (federal, state, and local)

- Screen for egregious financial history; for example, where adverse actions by creditors over time indicate a pattern of financial irresponsibility or where the applicant has taken on excessive debt or is involved in multiple disputes with creditors

The prescreening may be conducted as part of the pre-employment screening, but must be completed before the assignment of any personnel to a position requiring the aforementioned ADP/IT accesses. The pre-screening can be performed by the contractor's personnel security specialist, human resource manager, hiring manager or similar individual.

D. **Background Investigation Requirements.** Effective October 1, 2009, all requests for background investigations shall be submitted to OPM electronically in e-QIP. An interim DoD CAC can be given by the TMA PSD for access to DoD IT systems upon confirmation of a based on a favorable advance NAC, FBI fingerprint check, and an initiated background investigation in e-QIP.

III. ELECTRONIC QUESTIONNAIRES FOR INVESTIGATIONS PROCESSING (e-QIP)

A. **e-QIP Training and Access**.

(1) The Contractor FSO shall obtain the necessary training to access and use e-QIP.

(2) The Contractor FSO shall provide the following information to TMA PSD for e-QIP user accounts to be created:

- Social security number
- Full name
- Date of birth
- Place of birth

B. **e-QIP Role and Responsibilities.**

(1) The Contractor employee (also known as the applicant in the e-QIP process) shall:

- Be a US citizen
- Complete and submit the Optional Form (OF) 306, Declaration for Federal Employment to the Contractor FSO
- Complete the security questionnaire in e-QIP within 10 calendar days from the date of invitation by the Contractor FSO
- Sign the e-QIP signature forms provided by the Contractor FSO
- Provide fingerprints electronically or by using the FD 258, Fingerprint Card
- Complete and submit the TMA CAC request form to the Contractor FSO

(2) The Contractor FSO shall:

- Be a US citizen
- Be a contractor with a minimum investigation equivalent to a NACLC
- Provide the applicant with the appropriate processing forms to include the OF 306 and TMA CAC request form
- Initiate the applicant's security questionnaire in e-QIP
- Select the appropriate Agency Use Block (AUB) template in e-QIP
- Notify the COR by using e-mail that an e-QIP request has been initiated
- Inform the applicant to complete the security questionnaire in e-QIP within 10 calendar days
- Serve as the main Point of Contact (POC) for the applicant
- Monitor the e-QIP request, which includes ensuring the applicant completes the e-QIP request in designated time period
- Cancel or delete an e-QIP request on an applicant
- Request e-QIP golden question reset for applicants
- Print e-QIP signature form and obtain signature from the applicant
- Attach the OF 306 and signature forms in e-QIP before forwarding to TMA PSD for review
- Mail the applicant's original documents to include the signed e-QIP signature forms, the FD 258, and OF 306 to the TMA PSD
- Fax the TMA CAC request form and Add User form (when applicable) to

the TMA PSD

C. **Background Investigation Request for ADP/IT-I.**

(1) A background investigation request for an ADP/IT-I position must be approved by the Chief, TMA PSD.

(2) The Contracting Company shall submit a letter on company letterhead to the Chief, TMA PSD, which includes a complete job description of the position and the justification for the ADP/IT-I designation.

D. **Re-investigation Requirements.**

(1) Contractor personnel in ADP/IT-I and ADP/IT-II positions have re-investigation requirements. ADP/IT-I positions are re-investigated every 5 years. ADP/IT-II positions are re-investigated every 10 years. The re-investigation must be initiated within 60 days of the closed date of the prior investigation.

(2) The Contractor FSO shall track the re-investigation requirement for contractor employees. When a re-investigation is needed, the Contractor FSO shall:

- Initiate the contractor employee's security questionnaire in e-QIP
- Print contractor employee's e-QIP signature forms then obtain signatures
- Mail the e-QIP signature forms to the TMA PSD

E. **Reciprocal Acceptance of Prior Investigation.**

(1) If a new contractor personnel has a previous investigation, which meets the appropriate level of investigation required; and the break-in-service is 2 years or less, the investigation is reciprocally accepted, and no additional investigation is required.

(2) The Contracting Company shall request a verification of previous investigation from the TMA PSD, which includes the individual's name, social security number, and the closed date of the investigation. The notification may be sent to the TMA PSD by secure fax or by mail.

(3) The TMA PSD shall inform the Contractor FSO to confirm the acceptance of the previous investigation.

(4) The Contractor FSO shall notify the contractor personnel of the acceptance of the previous investigation.

F. **Notification of Employee Termination and Removal from DoD IT Systems Access.**

(1) The Contractor FSO shall notify the TMA PSD immediately when a contractor employee is terminated from a contract. The notification shall include the individual's name, the termination date, and if the individual's background investigation was initiated in e-QIP. Notification may be sent by mail, e-mail, or secure fax.

(2) The Contractor FSO shall:

- Forward a request to remove/delete the contractor employee's access to DoD IT systems
- Confiscate the DoD CAC from the contractor employee
- Return the DoD CAC to the TMA PSD.

G. **Requests for Additional Information.**

(1) OPM may request additional information while the contractor employee's investigation is in progress. The additional information must be provided to the TMA PSD by the specified date or the background investigation may be closed. If the background investigation is closed, interim access to all DoD IT systems will be terminated.

(2) The Defense Industrial Security Clearance Office (DISCO) or the Defense Office of Hearing and Appeals (DOHA) may request additional information during the adjudication process. The additional information must be provided within the specified timeframe or the adjudication process will be stopped. If the adjudication process is stopped, interim access to all DoD IT systems will be terminated.

H. **Non-US Citizens.** Non-US citizens are not being adjudicated for TRICARE trustworthiness determinations at this time. Non-US Citizens are not allowed access to DoD IT systems unless approved by an authority designated in Appendix 6, DoD 5200.2-R. Only US citizens shall be granted access and assigned to sensitive duties. Exceptions to these requirements shall be permitted only for compelling national security reasons (DoD 5200.2-R. C2.1.1, AP6.6.1).

I. **Notification and Mailing**. The Contractor shall use the following information to contact the TMA PSD. The Contractor shall ensure the safeguarding of any Personally Identifiable Information (PII) when transmitting any forms/documents to TMA PSD.

Mailing Address: TRICARE Management Activity

Office of Administration

Personnel Security Division
5111 Leesburg Pike
Skyline 5, Suite 810
Falls Church, VA 22041-3206

Secure Fax: (703) 681-3934

E-mail address: tma.psd@tma.osd.mil